Universidad de Valladolid

PROGRAMA DE DOCTORADO EN MATEMÁTICAS

TESIS DOCTORAL:

Commutative Algebra and Coding Theory, with Applications to Quantum Error-Correction

Presentada por Rodrigo San José Rubio para optar
al grado de Doctor por la Universidad de Valladolid

Dirigida por:
Philippe Gimenez
Diego Ruano

Abstract

Modern digital communication systems often face the challenge of data corruption due to noise, leading to discrepancies between transmitted and received symbols. Error-correcting codes guarantee reliable and fast transmission of information in such systems by adding redundant symbols. Algebraic Coding Theory plays an important role not only in many different aspects of communication but also in cryptography and quantum computing. This is because the additional algebraic structure of algebraic codes allows us to derive further properties of them. Since these properties characterize the performance of the code for certain applications, we can consider or design codes that are suitable for each setting. In particular, in this thesis we are interested in using tools from Commutative Algebra to derive properties of linear codes. We focus mainly on evaluation codes, since they have a natural connection to Commutative Algebra, but we also consider other types of codes such as cyclic codes (which can be viewed as subfield subcodes of evaluation codes) or matrix-product codes.

Many aspects of evaluation codes can be understood by means of the vanishing ideal of the set of points considered. A natural question that arises is how to compute this vanishing ideal. When one considers the evaluation points over the affine space, this computation is straightforward. However, in the projective setting one usually has to compute the radical of an ideal. In Paper A, we give an alternative and more efficient way of computing the vanishing ideal by using the saturation with respect to the homogeneous maximal ideal. Another option to study evaluation codes over the projective space is to consider a set of fixed representatives of the points, regarded as a subset of the affine space, and its vanishing ideal. In Papers B and C, we give a universal Gröbner basis for this vanishing ideal when the set of points corresponds to certain subsets of the projective line, or to the whole projective space.

Obtaining long codes with good parameters over a small finite field, which is desirable for applications, is a complicated problem in general. One approach to achieve this is to take codes with good parameters over a large field (e.g., Reed-Solomon codes), and then consider their subfield subcodes. The resulting code usually has lower dimension than the original code, and obtaining bases for the subfield subcodes (which give the dimension) is one of the main problems to study when working with subfield subcodes. By using the aforementioned Gröbner bases, in Papers B and C we obtain bases for the subfield subcodes of projective Reed-Solomon codes and projective Reed-Muller codes in many cases. An alternative approach for this problem is also given in Paper D, using a recursive construction for projective Reed-Muller codes.

The interest of the generalized Hamming weights of a linear code originates from the fact that they determine its performance on the wire-tap channel of type II. Since they

were introduced by Wei, many more applications have been found for them, such as list decoding or secret sharing schemes (considering relative generalized Hamming weights). In Paper D, we provide lower and upper bounds for the generalized Hamming weights of projective Reed-Muller codes, determining the true values in many cases. Inspired by the approach from Paper D, in Paper H we also provide bounds for the generalized Hamming weights of matrix-product codes. As a sample of our results, we obtain the exact value of the generalized Hamming weights of matrix-product codes obtained with two Reed-Solomon codes.

The development of reliable quantum computing and communication requires error-correction to deal with noise and decoherence. To perform error-correction, we can consider stabilizer quantum codes. The CSS construction provides a way to construct such codes using self-orthogonal classical linear codes. Furthermore, we consider two additional aspects specific to quantum codes: we can assume entanglement between the encoder and the decoder, giving rise to entanglement-assisted quantum error-correcting codes; and we can also consider two different types of errors, qudit-flip and phase-shift errors, leading to asymmetric quantum codes. The CSS construction can be generalized to cover these cases by considering a pair of classical linear codes, and their minimum distances. The dimension of their relative hull gives the parameter c, which is the minimum number required of maximally entangled pairs. Therefore, in this more general setting we do not require any self-orthogonality condition, but we have an additional parameter to compute. In Paper B, we have used the subfield subcodes of projective Reed-Solomon codes to construct both symmetric and asymmetric entanglement-assisted quantum error-correcting codes.

Since we have seen that the dimension of the hull determines the parameter c of the corresponding quantum code, the study of the hulls of projective Reed-Muller codes over the projective plane carried out in Paper E determines all the parameters of the corresponding quantum codes. Entanglement assistance can improve the rate of the corresponding quantum code, but maintaining entanglement over time can be costly. Therefore, this trade-off must be analyzed for each application, and this also motivates obtaining codes with different requirements of entanglement assistance. In Paper F, we study how to change the dimension of the hull of projective Reed-Muller codes by considering monomially equivalent codes, giving rise to families of codes with a flexible amount of entanglement.

One of the main problems for quantum computing is the fault-tolerant implementation of non-Clifford gates. In Paper G, we study CSS-T codes, which are quantum codes derived from the CSS construction that support the transversal T gate. We give a new characterization of CSS-T codes, and we use it to determine which CSS-T codes can be constructed from cyclic codes. Moreover, we also obtain a propagation rule for nondegenerate CSS-T codes, and we use it to obtain CSS-T codes with better parameters than those available in the literature.

Resumen

Los sistemas modernos de comunicación digital a menudo sufren de corrupción de datos debido al ruido, dando lugar a discrepancias entre los símbolos enviados y recibidos. Los códigos correctores de errores garantizan una transmisión fiable y rápida de la información en tales sistemas al agregar símbolos redundantes. La Teoría Algebraica de Códigos juega un papel importante en muchos aspectos diferentes de la comunicación, así como en la criptografía y la computación cuántica. Esto se debe a que la estructura algebraica adicional de los códigos algebraicos nos permite derivar propiedades adicionales de los mismos. Dado que estas propiedades caracterizan el rendimiento del código para ciertas aplicaciones, podemos considerar o diseñar códigos que sean adecuados para cada contexto. En particular, en esta tesis estamos interesados en usar herramientas de Álgebra Conmutativa para derivar propiedades de códigos lineales. Nos centramos principalmente en códigos de evaluación, ya que tienen una conexión natural con el Álgebra Conmutativa, pero también consideramos otros tipos de códigos como los códigos cíclicos (que pueden verse como subcódigos subcuerpo de los códigos de evaluación) o los códigos producto de matrices.

Muchos aspectos de los códigos de evaluación pueden entenderse mediante el ideal de anulación del conjunto de puntos considerado. Una pregunta natural que surge es cómo calcular este ideal de anulación. Cuando se consideran los puntos de evaluación sobre el espacio afín, este cálculo es sencillo. Sin embargo, en el caso proyectivo, generalmente se tiene que calcular el radical de un ideal. En el Artículo A, damos una forma alternativa y más eficiente de calcular el ideal de anulación utilizando la saturación con respecto al ideal homogéneo maximal. Otra opción para estudiar los códigos de evaluación sobre el espacio proyectivo es considerar un conjunto de representantes fijados de los puntos, considerados como un subconjunto del espacio afín, y su ideal de anulación. En los Artículos B y C, obtenemos una base de Gröbner universal para este ideal de anulación cuando el conjunto de puntos corresponde a ciertos subconjuntos de la recta proyectiva o a todo el espacio proyectivo.

Obtener códigos largos con buenos parámetros sobre un cuerpo finito pequeño, lo cual es deseable para aplicaciones, es un problema complicado en general. Una manera de lograr esto es considerar códigos con buenos parámetros sobre un cuerpo grande (por ejemplo, códigos Reed-Solomon), y luego considerar sus subcódigos subcuerpo. El código resultante generalmente tiene menor dimensión que el código original, y obtener bases para los subcódigos subcuerpo (lo cual también determina la dimensión) es uno de los principales problemas a estudiar cuando se trabaja con subcódigos subcuerpo. Utilizando las bases de Gröbner mencionadas anteriormente, en los Artículos B y C obtenemos bases para los subcódigos subcuerpo de los códigos Reed-Solomon proyectivos y los códigos Reed-Muller proyectivos en muchos casos. Un enfoque alternativo para este problema también

se presenta en el Artículo D, utilizando una construcción recursiva para los códigos Reed-Muller proyectivos.

El interés por los pesos de Hamming generalizados de un código lineal surge del hecho de que determinan su rendimiento en el canal *wire-tap* de tipo II. Desde que fueron introducidos por Wei, se han encontrado muchas más aplicaciones para ellos, como la decodificación en lista o los esquemas de compartición de secretos. En el Artículo D, proporcionamos cotas inferiores y superiores para los pesos de Hamming generalizados de los códigos Reed-Muller proyectivos, determinando los valores verdaderos en muchos casos. Generalizando las ideas del Artículo D, en el Artículo H también proporcionamos cotas para los pesos de Hamming generalizados de los códigos producto de matrices. Como muestra de nuestros resultados, obtenemos el valor exacto de los pesos de Hamming generalizados de los códigos producto de matrices obtenidos a partir dos códigos Reed-Solomon.

El desarrollo de la computación cuántica y la comunicación cuántica fiable requiere corrección de errores para lidiar con el ruido y la decoherencia. Para realizar la corrección de errores, podemos considerar códigos cuánticos estabilizadores. La construcción CSS proporciona una forma de construir dichos códigos utilizando códigos lineales clásicos auto-ortogonales. Además, consideramos dos aspectos adicionales específicos de los códigos cuánticos: podemos asumir entrelazamiento previo entre el codificador y el decodificador, dando lugar a códigos cuánticos de corrección de errores asistidos por entrelazamiento; y también podemos considerar dos tipos diferentes de errores, errores de *qudit-flip* y errores de *phase-shift*, lo que da lugar a los códigos cuánticos asimétricos. La construcción CSS se puede generalizar para cubrir estos casos considerando un par de códigos lineales clásicos y sus distancias mínimas. La dimensión de su *hull* relativo da el parámetro c, que es el número mínimo requerido de pares entrelazados maximalmente. Por lo tanto, en esta situación más general no requerimos ninguna condición de auto-ortogonalidad, pero tenemos un parámetro adicional que calcular. En el Artículo B, hemos utilizado los subcódigos subcuerpo de los códigos Reed-Solomon proyectivos para construir códigos cuánticos de corrección de errores asistidos por entrelazamiento tanto simétricos como asimétricos.

Dado que hemos visto que la dimensión del *hull* determina el parámetro c del código cuántico correspondiente, el estudio de los *hulls* de los códigos Reed-Muller proyectivos sobre el plano proyectivo realizado en el Artículo E determina todos los parámetros de los códigos cuánticos correspondientes. El entrelazamiento puede mejorar la tasa de transmisión del código cuántico correspondiente, pero mantenerlo a lo largo del tiempo puede ser costoso. Por lo tanto, este compromiso debe ser analizado para cada aplicación, y esto también motiva la obtención de códigos con diferentes requisitos de asistencia por entrelazamiento. En el Artículo F, estudiamos cómo cambiar la dimensión del *hull* de los códigos Reed-Muller proyectivos considerando códigos monomialmente equivalentes, dando lugar a familias de códigos cuánticos con requisitos flexibles de entrelazamiento.

Uno de los principales problemas para la computación cuántica es la implementación tolerante a fallos de puertas *non-Clifford*. En el Artículo G, estudiamos los códigos CSS-T, que son códigos cuánticos derivados de la construcción CSS que soportan la puerta transversal T. Damos una nueva caracterización de los códigos CSS-T, y la usamos para determinar qué códigos CSS-T pueden construirse a partir de códigos cíclicos. Además, obtenemos una regla de propagación para los códigos CSS-T no degenerados, y la usamos para obtener códigos CSS-T con mejores parámetros que los disponibles en la literatura.

Agradecimientos

En primer lugar, me gustaría expresar mi más profundo agradecimiento a mis directores de tesis, Philippe y Diego, cuya dedicación y compromiso han sido fundamentales para la culminación exitosa de esta tesis. Ellos me introdujeron a este tema de investigación, que encaja perfectamente dentro de mis intereses y conocimientos de álgebra y códigos (incluso de física). Su orientación no se ha limitado únicamente a proporcionarme los conocimientos necesarios, si no que ha cubierto otros aspectos esenciales, como la parte personal o incluso la gestión administrativa. También agradezco las oportunidades que me han brindado para realizar las distintas actividades que he llevado a cabo durante el doctorado.

I would also like to thank the members of the Applied Algebra Research Group at Virginia Tech for their hospitality during my stay(s). In particular, I would like to thank Gretchen, Hiram and Eduardo for our fruitful and pleasant discussions.

I am also grateful to Jade for inviting me to the Institute of Mathematics of Rennes and for revealing discussions.

Me gustaría dar las gracias a mi familia por su apoyo incondicional, y a mis amigos y compañeros de Valladolid. En particular, estoy agradecido a Jesús, cuyas conversaciones han sido una fuente inagotable de inspiración y reflexión durante el desarrollo de nuestras tesis.

Finalmente, también me gustaría agradecer el apoyo del Ministerio de Universidades por las becas FPU20/01311 y EST23/00777, que han financiado mis estudios de doctorado y mi estancia de investigación en Virginia Tech, y también quería agradecer el apoyo para financiar la asistencia a congresos, escuelas y talleres que me han dado los siguientes proyectos (a los cuales he tenido acceso gracias a mis directores): PID2019-104844GB-I00, PGC2018-096446-B-C21, TED2021-130358B-I00, PID2022-138906NB-C21, PID2022-137283NB-C22 y QCAYLE.

Rodrigo San José Rubio
Universidad de Valladolid, Julio de 2024

Contents

Part I

Introduction

Introduction

Linear codes, which were originally considered for reliable communication protocols, have found many different applications during the last few decades: secret sharing, post-quantum cryptography, quantum error-correction and quantum fault-tolerant computation, secure multiparty computation, etc. For each particular application, one needs to consider different aspects beyond the basic parameters of the codes involved. Two examples of these aspects of linear codes which are relevant to this thesis are the *generalized Hamming weights* and the *hulls* (for both the Euclidean and Hermitian inner products). One can impose additional structure on the codes considered to gain insight into these additional properties. A flexible framework for this purpose is provided by evaluation codes, which are obtained by evaluating functions at certain sets of points. Depending on the choice of functions and points, it is possible to use techniques from Algebraic Geometry and Commutative Algebra to study the properties of the codes involved.

In this thesis, we further explore the connections between *Commutative Algebra* and *Coding Theory*, with a particular focus on applications to quantum codes. This introduction provides an overview of the main results obtained during the development of the thesis, and it is organized according to several transversal topics which link the publications associated to this thesis together.

In Section 1, we introduce the main tools from Commutative Algebra that we use for the rest of the sections, which can be found in Papers A and C. In Section 2, we use the aforementioned tools to obtain bases for the subfield subcodes of projective Reed-Solomon codes and projective Reed-Muller codes. In Section 3, we obtain bounds for the generalized Hamming weights of projective Reed-Muller codes (Subsection 3.1) and matrix-product codes (Subsection 3.2). Finally, in Section 4, we derive quantum error-correcting codes appropriate for both quantum communication (Subsection 4.1) and fault-tolerant quantum computing (Subsection 4.2), using the results from Sections 1 and 2 (mainly for the case of quantum communication).

Since in Section 2 we consider several fields, mainly $\mathbb{F}_{q^s}$ and $\mathbb{F}_q$, we note now that all the codes are considered to be over $\mathbb{F}_q$, except in Section 2, where the original codes are considered over $\mathbb{F}_{q^s}$ and their subfield subcodes over $\mathbb{F}_q$. All the references from this chapter correspond to the global bibliography at the end of this thesis, which collects all the references mentioned in this introduction and in the publications.

1 Vanishing ideals and Coding Theory

We start this section by introducing evaluation codes, which are one of the main objects of study of this work. Let $\mathbb{F}_q$ be a finite field, let $R = \mathbb{F}_q[x_1, \ldots, x_m]$, and let $I \subset R$ be

an ideal. We denote by $\mathcal{X} = V_{\mathbb{F}_q}(I) = \{P_1, \ldots, P_n\} \subset \mathbb{A}^m$ the finite set of rational points in which all the polynomials of I vanish. We denote its vanishing ideal by $I(\mathcal{X})$, and we define the evaluation map

$$\mathrm{ev}_{\mathcal{X}} : R/I(\mathcal{X}) \to \mathbb{F}_q^n, \;\; f + I(X) \mapsto (f(P_1), \ldots, f(P_n)) \,.$$

This evaluation map provides an isomorphism of $\mathbb{F}_q$-vector spaces $R/I(\mathcal{X}) \cong \mathbb{F}_q^n$. We can consider L a vector subspace of $R/I(\mathcal{X})$ and define the *affine variety code* $C(I, L)$ as the image of L under the evaluation map $\mathrm{ev}_{\mathcal{X}}$. That is:

$$C(I, L) := \mathrm{ev}_{\mathcal{X}}(L) = \{\mathrm{ev}_{\mathcal{X}}(f + I(\mathcal{X})) \mid f + I(\mathcal{X}) \in L\}.$$

One of the key aspects of evaluation codes is that, since $\mathrm{ev}_{\mathcal{X}}$ is an isomorphism, we can identify the codewords of $C(I, L)$ with (classes of) polynomials. Thus, we can use polynomial-related techniques to gain information about the code $C(I, L)$.

Following a similar idea, one can consider evaluation codes over the projective space $\mathbb{P}^m$. Let $I \subset S = \mathbb{F}_q[x_0, \ldots, x_m]$ be a homogeneous ideal, and let $\mathbb{X} = V_{\mathbb{P}^m}(I) = \{[P_1], \ldots, [P_n]\} \subset \mathbb{P}^m$ be the finite set of projective points defined by I with representatives P_i. As before, if we denote the vanishing ideal of $\mathbb{X}$ by $I(\mathbb{X})$, we can define the following $\mathbb{F}_q$-linear map for each degree d:

$$\mathrm{ev}_d : S_d \to \mathbb{F}_q^n, \;\; f \mapsto \left(\frac{f(P_1)}{f_1(P_1)}, \ldots, \frac{f(P_n)}{f_n(P_n)} \right),$$

where $f_i \in S_d$ are fixed homogeneous polynomials satisfying $f_i(P_i) \neq 0$. The image of S_d under ev_d, denoted by $C_{\mathbb{X}}(d)$, is called a *projective Reed-Muller type code* of degree d on $\mathbb{X}$. By definition, $I(\mathbb{X})_d = \ker \mathrm{ev}_d$. Thus, $S_d/I(\mathbb{X})_d \cong C_{\mathbb{X}}(d)$. It can easily be checked that the basic parameters of the code (length, dimension and minimum distance) do not depend on the choice of the polynomials f_i. These codes have been studied in various contexts [27,28, 125] and they provide a nice connection between Coding Theory and Commutative Algebra [33, 60, 96, 131]. For example, the length of these codes is given by $n = \deg(S/I(\mathbb{X}))$, and the dimension is given by $k = H_{\mathbb{X}}(d) = \dim(S_d/I(\mathbb{X})_d)$. Furthermore, the minimum distance of $C_{\mathbb{X}}(d)$, and, more generally, its generalized Hamming weights (which we will introduce in later section), can also be expressed in terms of invariants of the ideal [33,96].

Therefore, the vanishing ideal $I(\mathbb{X})$ plays a crucial role in studying this family of codes. In many cases, the set of points $\mathbb{X}$ is usually given as the projective variety defined by a homogeneous ideal, and one may wonder how to compute $I(\mathbb{X})$ from this ideal. If we consider first an affine variety $\mathcal{X}$ defined by an ideal $I \subset R$ instead, the answer is straightforward. The ideal $I_q = I + I(\mathbb{A}^m) = I + \langle x_1^q - x_1, \ldots, x_m^q - x_m \rangle$ satisfies

$$V_{\overline{\mathbb{F}_q}}(I_q) = V_{\mathbb{F}_q}(I_q) = V_{\mathbb{F}_q}(I) = V_{\mathbb{F}_q}(I(X)) = \mathcal{X}.$$

By Seidenberg's Lemma [85, Prop. 3.7.15], I_q is radical. Hence, in this case $I_q = I(\mathcal{X})$ by Hilbert's Nullstellensatz (also see [55]).

We can replicate this idea in the projective case and consider, for a homogeneous ideal $I \subset S$, the ideal $I_q = I + I(\mathbb{P}^m)$, where

$$I(\mathbb{P}^m) = \langle \{x_i^q x_j - x_i x_j^q, 0 \leq i < j \leq m\} \rangle$$

was obtained in [99]. However, I_q is not radical in general. In fact, we have observed that this ideal is radical only in very specific cases. Since the computation of the radical of an ideal may be computationally intensive, this raises the question of finding easier ways to compute $I(\mathbb{X})$. In Paper A, we obtain the following result.

Theorem 1.1 [Thm. A.2.10]**.** *Let I be an homogeneous ideal such that $(I(\mathbb{P}^m) : I) \neq I(\mathbb{P}^m)$. Let $\mathbb{X} = V_{\mathbb{P}^m}(I)$ and $\mathfrak{m} = (x_0, \ldots, x_m)$ the homogeneous maximal ideal. Then*

$$I(\mathbb{X}) = (I + I(\mathbb{P}^m)) : \mathfrak{m}^\infty.$$

The condition $(I(\mathbb{P}^m) : I) \neq I(\mathbb{P}^m)$ is equivalent to having $\mathbb{X} \neq \emptyset$, which is the case we are interested in for Coding Theory. Thus, this result provides a more efficient way of computing $I(\mathbb{X})$ by using the saturation with respect to the homogeneous maximal ideal instead of computing the radical, since the saturation is regarded as a less computationally intensive operation than obtaining the radical.

Another approach to study Reed-Muller type codes is to fix the representatives of the points of $\mathbb{P}^m$. Indeed, we can fix the *standard representatives*, that is, for each point in $\mathbb{P}^m$, we consider the representative with the leftmost nonzero coordinate equal to 1. In this way, we obtain a set of representatives, denoted P^m, which can be regarded as a subset of $\mathbb{A}^{m+1}$. Analogously, from $\mathbb{X} \subset \mathbb{P}^m$ we obtain its set of standard representatives $X \subset P^m \subset \mathbb{A}^{m+1}$. We can extend the definition of ev_X to S, and then we can consider the code $\mathrm{ev}_X(S_d)$, which is monomially equivalent to $C_{\mathbb{X}}(d)$. This gives the isomorphism

$$\mathrm{ev}_X(S_d) \cong S_d/(I(X) \cap S_d) \cong (S_d + I(X))/I(X),$$

and we can also study the properties of the code $\mathrm{ev}_X(S_d)$ (or $C_{\mathbb{X}}(d)$) by studying the ideal $I(X)$. To compute $I(X)$, first we consider $I(P^m)$, for which we have the following result from Paper C.

Theorem 1.2 [Thm. C.4.1]**.** *The vanishing ideal of P^m is generated by:*

$$\begin{aligned} I(P^m) =& \langle x_0^2 - x_0, x_1^q - x_1, x_2^q - x_2, \ldots, x_m^q - x_m, (x_0 - 1)(x_1^2 - x_1), \\ & (x_0 - 1)(x_1 - 1)(x_2^2 - x_2), \ldots, (x_0 - 1) \cdots (x_{m-1}^2 - x_{m-1}), (x_0 - 1) \cdots (x_m - 1) \rangle. \end{aligned}$$

Moreover, these generators form a universal Gröbner basis of the ideal $I(P^m)$, and we have that

$$\mathrm{in}(I(P^m)) = \langle x_0^2, x_1^q, x_2^q, \ldots, x_m^q, x_0 x_1^2, x_0 x_1 x_2^2, \ldots, x_0 x_1 \cdots x_{m-1}^2, x_0 x_1 \cdots x_m \rangle.$$

With this result, we can argue as before and, if we consider a homogeneous ideal I such that $V_{\mathbb{F}_q}(I) = \mathbb{X}$, then $I_q = I + I(P^{m-1})$ is radical by Seidenberg's Lemma [85, Prop. 3.7.15], and $I_q = I(X)$ (again, also see [55]).

The most well known family of projective Reed-Muller type codes are obtained when one considers $X = P^m$. In that case, the code $\mathrm{ev}_X(S_d)$ is called a *projective Reed-Muller code* of degree d, and is denoted by $\mathrm{PRM}_d(q, m)$, or by $\mathrm{PRM}_d(m)$ if there is no confusion about the field. This family of codes was introduced in [88], and their basic parameters were studied in [125]. In particular, from [125] we have the following results (for the minimum distance, also see [56, 126]).

Theorem 1.3. *The projective Reed-Muller code* $\mathrm{PRM}_d(q,m)$, $1 \leq d \leq m(q-1)$, *is an* $[n,k]$*-code with*

$$n = \frac{q^{m+1}-1}{q-1},$$
$$k = \sum_{t \equiv d \bmod q-1, 0<t\leq d} \left(\sum_{j=0}^{m+1} (-1)^j \binom{m+1}{j} \binom{t-jq+m}{t-jq} \right).$$

For the minimum distance, we have

$$\mathrm{wt}(\mathrm{PRM}_d(q,m)) = (q-\ell)q^{m-r-1}, \text{ where } d-1 = r(q-1)+\ell,\ 0 \leq \ell < q-1.$$

Theorem 1.4. *Let* $1 \leq d \leq m(q-1)$ *and let* $d^\perp = m(q-1)-d$. *Then*

$$\mathrm{PRM}_d^\perp(q,m) = \mathrm{PRM}_{d^\perp}(q,m) \qquad \text{if } d \not\equiv 0 \bmod q-1,$$
$$\mathrm{PRM}_d^\perp(q,m) = \mathrm{PRM}_{d^\perp}(q,m) + \langle (1,\ldots,1) \rangle \qquad \text{if } d \equiv 0 \bmod q-1.$$

In [89], it is shown that the parameters of projective Reed-Muller codes can outperform those of affine Reed-Muller codes. However, projective Reed-Muller codes have received much less attention than their affine counterpart, and a substantial part of this thesis is devoted to filling this gap.

To study $\mathrm{PRM}_d(m)$, we study first how to work over the quotient ring $S/I(P^m)$, which contains $(S_d + I(P^m))/I(P^m) \cong \mathrm{PRM}_d(m)$. From Macaulay's classical result [42, Thm. 15.3], the monomials not contained in $\mathrm{in}(P^m)$ (sometimes called the *footprint*) form a basis for $S/I(P^m)$. Therefore, using Theorem 1.5, in Paper C we obtain the following basis.

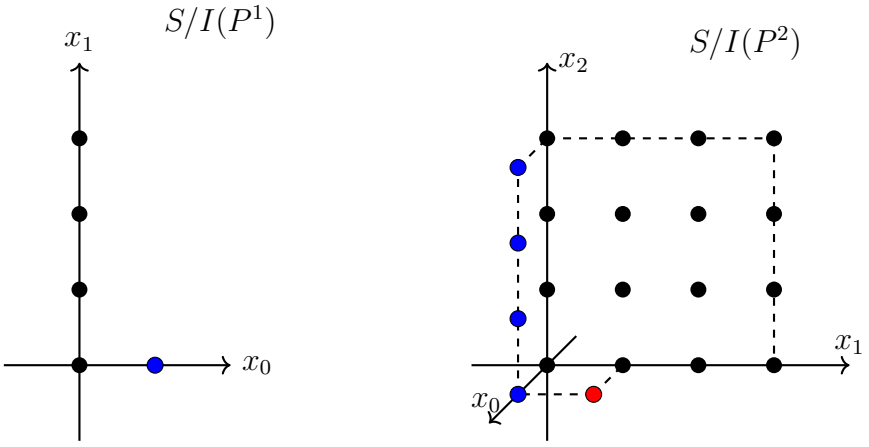
Lemma 1.5 [Lem. C.4.3]**.** *The set given by the classes of the following monomials*

$$\{x_1^{a_1} \cdots x_m^{a_m}, x_0 x_2^{a_2} \cdots x_m^{a_m}, \ldots, x_0 x_1 \cdots x_{m-2} x_m^{a_m}, x_0 \cdots x_{m-1} \mid 0 \leq a_i \leq q-1, 1 \leq i \leq m\}$$

is a basis for $S/I(P^m)$.

One can check that there are exactly $q^m + q^{m-1} + \cdots + q + 1 = (q^{m+1}-1)/(q-1) = |P^m|$ monomials in the basis.

Example 1.6. We have $\mathrm{in}(I(P^1)) = \langle x_1^2, x_2^q, x_1 x_2 \rangle$ and $\mathrm{in}(I(P^2)) = \langle x_1^2, x_2^q, x_3^q, x_1 x_2^2, x_1 x_2 x_3 \rangle$. For $q = 4$, we have the following footprints:



We have used different colors to show the correspondence between the number of monomials in the footprint and $|P^m|$. For $m = 2$ and $q = 4$, we obtain $4^2 = 16$ monomials in black, which is the number of points of $\mathbb{A}^2$, and $4 + 1 = 5$ monomials in blue or red, corresponding to the line at infinity, which can be regarded as an affine line (monomials in blue) and a point at infinity (monomial in red).

Additionally, in Theorem C.4.4, we prove how to reduce any monomial with respect to the Gröbner basis from Theorem 1.2, thus obtaining its expression in terms of the basis from Lemma 1.5. These are the main tools we use to study projective Reed-Muller codes and to obtain applications in the following sections.

2 Subfield subcodes

Given a code $C \subset \mathbb{F}_{q^s}^n$, its subfield subcode is the linear code $C \cap \mathbb{F}_q^n$, which we denote C_q (it can be denoted by C^σ as well). Considering subfield subcodes is a standard technique for constructing long linear codes over a small finite field. For instance, BCH codes can be seen as subfield subcodes of Reed-Solomon codes [13]. In the multivariate case, the subfield subcodes of J-affine variety codes are well known [47] (in particular, the subfield subcodes of Reed-Muller codes) and have been used for several applications [46, 52]. The main problem that arises when working with subfield subcodes is the computation of a basis for the code, which also gives the dimension. In this section, we study the subfield subcodes of projective Reed-Solomon codes, which can be regarded as doubly extended BCH codes, and projective Reed-Muller codes. Throughout this section, the polynomial rings are understood to have coefficients in $\mathbb{F}_{q^s}$, and the codes are understood to be over $\mathbb{F}_{q^s}$ except when considering subfield subcodes, which are assumed to be over $\mathbb{F}_q$.

We introduce first projective Reed-Solomon codes. We consider $X \subset P^1$ (over $\mathbb{F}_{q^s}$), and the polynomial ring $S = \mathbb{F}_{q^s}[x_0, x_1]$. Given $\Delta \subset \{0, 1, \ldots, n-1\}$, we define $d(\Delta) := \max\{i \mid i \in \Delta\}$. The *projective Reed-Solomon* code associated to Δ and X is the code generated by

$$\{\mathrm{ev}_X(x_0^{d(\Delta)-i} x_1^i) \mid i \in \Delta\},$$

which will be denoted by $\mathrm{PRS}(X, \Delta)$. Given a degree $1 \leq d \leq q^s$, the most standard definition of projective Reed-Solomon code in the literature is the code $\mathrm{PRS}(P^1, \Delta_d)$, where $\Delta_d := \{0, 1, \ldots, d\}$. The code $\mathrm{PRS}(P^1, \Delta_d)$ is also called *doubly extended Reed-Solomon code* and its parameters are $[q^s + 1, d + 1, q^s - d + 1]$. This code can be regarded as a projective Reed-Muller code in 1 variable.

For the evaluation points X, we are going to consider a subgroup of the multiplicative group $\mathbb{F}_{q^s}^*$, plus zero and the point at infinity. Indeed, given N such that $N - 1 \mid q^s - 1$, we define Y_N to be the zero locus of $\langle x^N - x \rangle$, that is, a multiplicative subgroup of $\mathbb{F}_{q^s}^*$ plus zero, and $X_N = (\{1\} \times Y_n) \cup \{(0, 1)\} \subset P^1$. For convenience, we will denote $\mathrm{PRS}(N, \Delta) := \mathrm{PRS}(X_N, \Delta)$. With this notation, doubly extended Reed-Solomon codes are denoted by $\mathrm{PRS}(q^s, \Delta_d)$. In general, for the codes $\mathrm{PRS}(N, \Delta)$ we have the parameters $[N + 1, |\Delta|, \geq N - d(\Delta) + 1]$.

We will say that a polynomial evaluates to $\mathbb{F}_q$ in X if $\mathrm{ev}_X(f) \in \mathbb{F}_q^n$. The following result, which partially appears in Papers B and C, is crucial for relating the subfield subcodes of codes over the affine space and the projective space.

Lemma 2.1 [Lem. B.3.1 and Lem. C.2.6]. *Let $X_N \subset P^1$. Then $f \in \mathbb{F}_{q^s}[x_0, x_1]$ evaluates to $\mathbb{F}_q$ in $X_N \iff f(1, x_1)$ evaluates to $\mathbb{F}_q$ in Y_N and $f(0, 1)$ is in $\mathbb{F}_q$. For the case $m \geq 2$, one has that $f \in \mathbb{F}_{q^s}[x_0, \ldots, x_m]$ evaluates to $\mathbb{F}_q$ in P^m if and only if $f(1, x_1, \ldots, x_m)$, $f(0, 1, x_2, \ldots, x_m)$, $f(0, 0, 1, x_3, \ldots, x_m), \ldots$, and $f(0, 0, \ldots, 0, 1, x_m)$ evaluate to $\mathbb{F}_q$ in $\mathbb{A}^m, \mathbb{A}^{m-1}, \mathbb{A}^{m-2}, \ldots, \mathbb{A}$, respectively, and $f(0, \ldots, 0, 1) \in \mathbb{F}_q$.*

Since bases for subfield subcodes of Reed-Solomon codes and the subfield subcodes of affine Reed-Muller codes are known [47], by homogenizing those polynomials we get candidates for polynomials that evaluate to $\mathbb{F}_q$ in the projective space, because the homogenization will automatically satisfy that, when setting $x_0 = 1$, the resulting polynomial evaluates to $\mathbb{F}_q$ (the first condition in Lemma 2.1 for both P^1 and P^m). For simplicity, we show next how to use this Lemma to obtain bases for the subfield subcodes of projective Reed-Solomon codes only. The details for the case of projective Reed-Muller codes are in Paper C. First, we need to introduce the notation of cyclotomic sets and trace functions.

For N such that $N - 1 \mid q^s - 1$, we define $\mathbb{Z}_N = \{0\} \cup \mathbb{Z}/\langle N - 1\rangle$, where we represent the classes of $\mathbb{Z}/\langle N - 1\rangle$ by $\{1, \ldots, N\}$. A subset $\mathfrak{I}$ of $\mathbb{Z}_N$ is called a *cyclotomic set* with respect to q if $q \cdot z \in \mathfrak{I}$ for any $z \in \mathfrak{I}$. $\mathfrak{I}$ is said to be minimal (with respect to q) if it can be expressed as $\mathfrak{I} = \{q^i \cdot z, i = 1, 2, \ldots\}$ for a fixed $z \in \mathfrak{I}$, and in that situation we will write $\mathfrak{I}_z := \mathfrak{I}$ and $n_z = |\mathfrak{I}_z|$. We say z is a *minimal representative* of $\mathfrak{I}_z$ if z is the least element in $\mathfrak{I}_z$, and we will say it is a *maximal representative* of $\mathfrak{I}_z$ if it is the biggest element. We will denote by $\mathcal{A}$ the set of minimal representatives of the minimal cyclotomic cosets, and by $\mathcal{B}$ the set of maximal representatives of the minimal cyclotomic cosets.

Given a degree d and a polynomial $f(x_1) \in \mathbb{F}_{q^s}[x_1]$ with $\deg(f) \leq d$, its homogenization up to degree d is the homogeneous polynomial $f^h(x_0, x_1) := x_0^d f(x_1/x_0) \in \mathbb{F}_{q^s}[x_0, x_1]_d$. For each $a \in \mathcal{A}$, we define the following trace map:

$$\mathcal{T}_a : \mathbb{F}_{q^s}[x_1]/I(Y_N) \to \mathbb{F}_{q^s}[x_1]/I(Y_N), \;\; f \mapsto f + f^q + \cdots + f^{q^{(n_a-1)}},$$

and given $\Delta \subset \{0, 1, \ldots, N-1\}$, we denote $\Delta_{\mathfrak{I}} := \bigcup_{\mathfrak{I}_a \subset \Delta} \mathfrak{I}_a \subset \Delta$.

Consider $f \in \mathbb{F}_q[x_1]$. We choose for $\mathcal{T}_a(f)$ the representative of the class in $\mathbb{F}_{q^s}[x_1]/I(Y_N)$ which has the exponents of each monomial reduced modulo $q^s - 1$. Given $d \geq 1$, if the degree of $\mathcal{T}_a(f)$ is lower than or equal to d, then we define $\mathcal{T}_a^h(f) := (\mathcal{T}_a(f))^h$. With this notation, in Paper B we obtain the following basis for $\mathrm{PRS}(N, \Delta)_q$.

Theorem 2.2 [Thm. B.3.4]. *Let $N \mid q^s - 1$, let Δ be a nonempty subset of $\{0, 1, \ldots, N-1\}$, and let $d = d(\Delta)$. Set ξ_b a primitive element of the field $\mathbb{F}_{q^{n_b}}$. A basis for $\mathrm{PRS}(N, \Delta)_q$ is given by the image by ev_{X_N} of the following polynomials.*

If $\mathfrak{I}_d \subset \Delta$:

$$\bigcup_{b \in \mathcal{B} \mid \mathfrak{I}_b \subset \Delta, b < d} \{\mathcal{T}_b^h(\xi_b^r x_1^b) \mid 0 \leq r \leq n_b - 1\} \cup \{\mathcal{T}_d^h(x_1^d)\}.$$

If $\mathfrak{I}_d \not\subset \Delta$:

$$\bigcup_{b \in \mathcal{B} \mid \mathfrak{I}_b \subset \Delta} \{\mathcal{T}_b^h(\xi_b^r x_1^b) \mid 0 \leq r \leq n_b - 1\}.$$

As a corollary, one can deduce a formula for the dimension of these subfield subcodes.

Corollary 2.3 [Cor. B.3.7]. *The dimension of* $\mathrm{PRS}(N,\Delta)_q$ *is the following:*

$$\dim \mathrm{PRS}(N,\Delta)_q = \begin{cases} \sum_{b\in\mathcal{B}:\mathfrak{I}_b\subset\Delta} n_b - (n_d-1) = \sum_{b\in\mathcal{B}:\mathfrak{I}_b\subset\Delta, b<d} n_b + 1 & \text{if } \mathfrak{I}_d \subset \Delta \\ \sum_{b\in\mathcal{B}:\mathfrak{I}_b\subset\Delta} n_b & \text{otherwise} \end{cases}$$

For the minimum distance, since $\mathrm{PRS}(N,\Delta)_q \subset \mathrm{PRS}(N,\Delta)$, we always have

$$\mathrm{wt}(\mathrm{PRS}(N,\Delta)_q) \geq N - d(\Delta) + 1.$$

For some applications (e.g., for quantum codes) it is useful to also have a basis for the dual of the code. The following result is due to Delsarte [38] and is often used to study the dual of subfield subcodes.

Theorem 2.4. *Let* $C \subset \mathbb{F}_{q^s}^n$ *be a linear code.*

$$C_q^\perp = (C \cap \mathbb{F}_q^n)^\perp = \mathrm{Tr}(C^\perp),$$

where $\mathrm{Tr} : \mathbb{F}_{q^s} \to \mathbb{F}_q$ *maps* x *to* $x + x^q + \cdots + x^{q^{s-1}}$ *and is applied componentwise to* $C^\perp$.

The dual of $\mathrm{PRS}(N,\Delta)$ is studied in Paper B. We show that $\mathrm{PRS}(N,\Delta)^\perp$ is not generated by the evaluation of some monomials unless $p \mid N$ (where p is the characteristic of $\mathbb{F}_{q^s}$) or $\mathrm{wt}(\mathrm{PRS}(N,\Delta)) = 1$. For the case $p \mid N$, we obtain a basis for $\mathrm{PRS}(N,\Delta)^\perp$ in Proposition B.4.10. This result, together with Delsarte's theorem, allows us to obtain a basis for $(\mathrm{PRS}(N,\Delta)_q)^\perp$ in Theorem B.4.14.

Following the ideas from [53], we can evaluate at the zeroes of a trace (plus the point at infinity). In that case, instead of having a formula for the dimension, we only have a lower bound, which gives room for improvements in some cases. Indeed, by doing this, in Paper B, we obtain codes with parameters $[129, 90, 15]_4$, $[129, 86, 16]_4$ and $[129, 41, 44]_4$. In [64], a construction for a code with parameters $[129, 86, 16]_4$ is missing, and the parameters $[129, 90, 15]_4$ and $[129, 41, 44]_4$ exceed the best known values. By shortening and puncturing, we obtain 22 new codes in total, whose parameters improve the ones in the table or whose construction was missing.

For the case of projective Reed-Muller codes, for $m = 2$ we obtain explicit bases for their subfield subcodes and for the duals thereof in Paper C. To understand the linear independence of the evaluation of the polynomials involved, the crucial tool is considering the normal form of these polynomials with respect to the Gröbner basis from Theorem 1.2. When increasing m, the computations get increasingly involved. We give now a complementary approach, using the recursive construction from Paper D, which allows us to obtain bases for the subfield subcodes of projective Reed-Muller codes for any m for some particular degrees. We start with the aforementioned recursive construction. We denote by $\mathrm{RM}_d(m)$ the affine Reed-Muller code of degree obtained by evaluating the polynomials of degree $\leq d$ in m variables.

Theorem 2.5 [Thm. D.3.1]. *Let* $1 \leq d \leq m(q^s - 1)$ *and let* ξ *be a primitive element in* $\mathbb{F}_{q^s}$. *We have the following recursive construction:*

$$\mathrm{PRM}_d(m) = \{(u + v_{\xi,d}, v) \mid u \in \mathrm{RM}_{d-1}(m), v \in \mathrm{PRM}_d(m-1)\},$$

where $v_{\xi,d} := v \times \xi^d v \times \cdots \times \xi^{(q^s-2)d} v \times \{0\} = (v, \xi^d v, \xi^{2d} v, \ldots, \xi^{(q^s-2)d} v, 0)$.

This is reminiscent of what happens with binary Reed-Muller codes, which can be constructed recursively using the $(u, u+v)$ construction. Also note that, more generally, q-ary Reed-Muller codes can be constructed recursively using a matrix-product code construction [16]. For some particular degrees, this construction translates for the subfield subcodes.

Corollary 2.6 [Cor. D.4.2]**.** *Let $\xi \in \mathbb{F}_{q^s}$ be a primitive element. Let $m > 1$ and let $d_\lambda = \lambda\frac{q^s-1}{q-1}$ for some $\lambda \in \{1, 2, \ldots, m(q-1)\}$. Then we have*

$$(\mathrm{PRM}_{d_\lambda}(m))_q = \{(u + v_{\xi,d_\lambda}, v), u \in (\mathrm{RM}_{d_\lambda-1}(m))_q, v \in (\mathrm{PRM}_{d_\lambda}(m-1))_q\}.$$

As a consequence, we obtain:

$$\dim((\mathrm{PRM}_{d_\lambda}(m))_q) = \dim((\mathrm{RM}_{d_\lambda-1}(m))_q) + \dim((\mathrm{PRM}_{d_\lambda}(m-1))_q).$$

We see that, for those particular degrees, we obtain the dimension of the subfield subcode in a recursive manner. The dimension of the subfield subcodes of affine Reed-Muller codes is known, and the formula can be applied recursively until it depends on the projective Reed-Muller codes over $\mathbb{P}^2$ or $\mathbb{P}^1$, for which we know the dimension of their subfield subcodes by Papers B and C. In a similar recursive way, it is also possible to derive a basis for $(\mathrm{PRM}_{d_\lambda}(m))_q$ from bases of subfield subcodes of affine Reed-Muller codes (which are known [47]) and subfield subcodes of projective Reed-Muller codes in less variables.

In Table 1 we show the parameters of some subfield subcodes of projective Reed-Muller codes. All codes presented in Table 1 exceed the Gilbert-Varshamov bound, and some of them have the best known parameters according to [64]. More examples can be found in Papers C and D.

Table 1: Parameters of some subfield subcodes of projective Reed-Muller codes arising from the recursive construction.

q	s	m	λ	n	k	$\mathrm{wt}(C) \geq$
2	2	2	1	21	9	8
2	2	3	1	85	16	32
2	2	3	2	85	60	8
3	9	2	1	91	9	54
4	2	2	1	273	9	192
5	2	2	1	651	9	500
7	2	2	1	2451	9	2058

3 Generalized Hamming weights

The generalized Hamming weights (GHWs) of a code, introduced in [132], are a set of parameters that generalizes the minimum distance of a code. As such, they give finer information about the code, and, in terms of applications, they characterize the performance of the code on the wire-tap channel of type II and as a t-resilient function [132], and they also have applications to list decoding [62, 69]. Moreover, for certain families of codes, they are interesting by themselves, e.g., for projective Reed-Muller codes, they

give the maximum number of solutions of a system of homogeneous polynomial equations in the projective space over a finite field. In this thesis, we have studied the GHWs of projective Reed-Muller codes and matrix-product codes (which we will define later).

To introduce the GHWs of a code, we first start with the notion of support. Let $C \subset \mathbb{F}_q^n$, and let $D \subset C$ be a subcode. The support of D, denoted by $\mathrm{supp}(D)$, is defined as

$$\mathrm{supp}(D) := \{i \mid \exists\ u = (u_1, \ldots, u_n) \in D,\ u_i \neq 0\}.$$

The r-th *generalized Hamming weight* of C, denoted by $d_r(C)$, is defined as

$$d_r(C) := \min\{|\mathrm{supp}(D)| \mid D \text{ is a subcode of } C \text{ with } \dim D = r\}.$$

Remark 3.1. Note that we use the notation $d_r(C)$ for the r-th generalized Hamming weight, and d_i for some particular degree (depending on i) in some results. There is no confusion between the two notations since $d_r(C)$ always makes reference to the code C.

For ease of notation, throughout this thesis we will denote $d_0(C) = 0$, and $d_r(C) = \infty$ if $r > \dim C$. The GHWs satisfy the following general properties for any linear code C, as shown in [132].

Theorem 3.2 (Monotonicity)**.** *For an $[n, k]$ linear code C with $k > 0$ we have*

$$1 \leq d_1(C) < d_2(C) < \cdots < d_k(C) \leq n.$$

Corollary 3.3 (Generalized Singleton Bound)**.** *For an $[n, k]$ linear code C we have*

$$d_r(C) \leq n - k + r,\ 1 \leq r \leq k.$$

Remark 3.4. As a consequence of the previous results, for an MDS code C we have

$$d_r(C) = n - k + r,$$

for all $1 \leq r \leq k$.

In the following subsections, we show the results we have obtained in Papers D and H regarding the GHWs of projective Reed-Muller codes and matrix-product codes.

3.1 GHWs of projective Reed-Muller codes

The GHWs of affine Reed-Muller codes were completely determined more than 20 years ago in [72]. However, the computation of the GHWs of projective Reed-Muller codes in general remains an open problem and only partial results are known [9, 17, 36]. In [11], many of the previous results and hypotheses are collected, and the authors obtain the GHWs of projective Reed-Muller codes in some cases for degree $d < q$. In Paper D, we use the recursive construction from Theorem 2.5 to give a recursive lower bound for the GHWs of a projective Reed-Muller code of any degree, which we show next (note that we use q instead of q^s, which is what we used in Section 2 since we were considering subfield subcodes).

Theorem 3.5 [Thm. D.5.7]. *Let $1 \leq d \leq m(q-1)$ and $2 \leq r \leq \dim(\mathrm{PRM}_d(m))$. We consider*

$$Y = \left\{ (\alpha, \gamma) : \begin{array}{c} \max\{r - \dim \mathrm{RM}_{d-1}(m), 0\} \leq \alpha \leq \min\{\dim \mathrm{PRM}_d(m-1), r\} \\ \max\{r - \dim \mathrm{RM}_d(m), 0\} \leq \gamma \leq \min\{\dim \mathrm{PRM}_{d-(q-1)}(m-1), \alpha\} \end{array} \right\}.$$

Then we have

$$d_r(\mathrm{PRM}_d(m)) \geq \min_{(\alpha,\gamma)\in Y} B_{\alpha,\gamma},$$

where $B_{\alpha,\gamma}$ is defined as

$$\begin{aligned} B_{\alpha,\gamma} := &\max(d_{r-\gamma}(\mathrm{RM}_d(m)), d_{r-\alpha}(\mathrm{RM}_{d-1}(m))) \\ &+ \max(d_\alpha(\mathrm{PRM}_d(m-1)), d_\gamma(\mathrm{PRM}_{d-(q-1)}(m-1))). \end{aligned}$$

We say that the bound is recursive because it bounds the GHWs of $\mathrm{PRM}_d(m)$ using the GHWs of affine Reed-Muller codes (which are known [72]), and the GHWs of projective Reed-Muller codes in less variables. For $m = 1$, projective Reed-Muller codes are doubly extended Reed-Solomon codes, which are MDS and, thus, we know their GHWs by Remark 3.4. With the GHWs of doubly extended Reed-Solomon codes, we can bound the GHWs of projective Reed-Muller codes over $\mathbb{P}^2$, which can be used to bound the GHWs for $\mathbb{P}^3$, etc. There is another bound for the GHWs of projective Reed-Muller codes, the projective footprint bound, which is a generalization of the well known footprint bound to the projective case [10, 96]. In all the cases we have checked, the bound from Theorem 3.5 is greater than or equal to the projective footprint bound, and in many cases it is strictly greater. Moreover, the bound from Theorem 3.5 has proven to be much less computationally intensive to compute in our experiments than the projective footprint bound.

Since this result mainly depends on the recursive construction from Theorem 2.5, in Paper D we also use Theorem 2.6 to obtain a recursive bound for the GHWs of the subfield subcodes of projective Reed-Muller codes for some degrees.

To complement the lower bound from Theorem 3.5, we obtain the following upper bound.

Lemma 3.6 [Lem. D.5.8]. *Let $2 \leq r \leq \max\{\dim \mathrm{RM}_{d-1}(m), \dim \mathrm{PRM}_d(m-1)\}$ and $1 \leq d \leq m(q-1)$. Then*

$$d_r(\mathrm{PRM}_d(m)) \leq \min\{d_r(\mathrm{RM}_{d-1}(m)), q \cdot d_r(\mathrm{PRM}_d(m-1))\}.$$

Note that the previous result only gives a nontrivial bound if $r \leq \dim \mathrm{RM}_{d-1}(m)$ or $r \leq \dim \mathrm{PRM}_d(m-1)$. This upper bound, together with the monotonicity of the GHWs 3.2, allows us to obtain a criterion for verifying that the bound from Theorem 3.5 is sharp in many cases. In Table 2, we show the values we obtain for $q = 4$ and $m = 2$. We use dots when the GHWs grow by one unit when increasing r by one unit (note that, for these values, we obtain the exact value of the GHWs). Thus, with the general properties of the GHWs and our bounds, we obtain the exact value of the GHWs, except in 6 cases.

This table can be improved by considering the following result from [132].

Theorem 3.7 (Duality). *Let C be an $[n, k]$ code. Then*

$$\{d_r(C) : 1 \leq r \leq k\} = \{1, 2, \ldots, n\} \setminus \{n + 1 - d_r(C^\perp) : 1 \leq r \leq n - k\}.$$

Table 2: Generalized Hamming weights for $q = 4$, $m = 2$.

$d\backslash r$	2	3	4	5	6	7	8	9	10	11	$\cdots$	20
1	20	21										
2	15	16	19	20	21							
3	10-11	11-12	14	15	16	18	19	20	21			
4	5-7	8	9-10	10-11	12	13	14	15	16	17	$\cdots$	
5	4	5-6	7	8	9	10	11	12	13	14	$\cdots$	
6	3	4	5	6	7	8	9	10	11	12	$\cdots$	21

The set $\{d_r(C) : 1 \leq r \leq k\}$ is called the weight hierarchy of the code C. From Theorem 3.7 we see that the weight hierarchy of a code is completely determined by the weight hierarchy of its dual, and vice versa. Since we know that, for $d \not\equiv 0 \bmod q-1$, the dual of a projective Reed-Muller code is also a projective Reed-Muller code by Theorem 1.4, for a given code $\mathrm{PRM}_d(m)$ we can apply our bounds to its dual code and obtain additional information about the weight hierarchy of $\mathrm{PRM}_d(m)$. In this way, for the case $d \not\equiv 0 \bmod q-1$, we improve the values from Table 2 to the ones in Table 3. We note that we obtain the exact value of all the GHWs with $d \not\equiv 0 \bmod q-1$ in this case. Further examples can be found in Paper D.

Table 3: Improved table of the generalized Hamming weights for $q = 4$, $m = 2$, with $d \not\equiv 0 \bmod q-1$.

$d\backslash r$	2	3	4	5	6	7	8	9	10	11	$\cdots$	18
1	20	21										
2	15	16	19	20	21							
4	5	8	9	11	12	13	14	15	16	17	$\cdots$	
5	4	5	7	8	9	10	11	12	13	14	$\cdots$	21

3.2 GHWs of matrix-product codes

Matrix-product codes (MPCs) were introduced by Blackmore and Norton in [16]. These codes have been object of study for many different applications [50, 51, 92, 93]. From the properties of the constituent codes, one can derive properties of the corresponding MPC. Most notably, one can obtain a lower bound for the minimum distance of the MPC from the minimum distances of the constituent codes [16], but one can also derive self-orthogonality properties for some matrices [51, 81, 95] or decoding algorithms [73, 74, 77].

The aim of this subsection is to study the GHWs of a MPC in terms of those of its constituent codes. By doing this, one can consider families of codes with known GHWs, and derive different codes with bounded GHWs using the MPC construction. This allows us to substantially expand the families of codes for which we have bounds for their GHWs. Some of the results of in subsection are reminiscent of the results from Section 3.1, since the techniques are inspired by the ones used in Paper D. This is mainly due to the fact that the recursive construction from Theorem 2.5 resembles the $(u, u+v)$ construction, a particular case of a matrix-product code construction. We start by defining MPCs as in [16].

Definition 3.8. Let $C_1, \ldots, C_\ell \subset \mathbb{F}_q^n$ be linear codes of length n, which we call *constituent codes*, and let $A = (a_{ij}) \in \mathbb{F}_q^{\ell \times h}$ be an $\ell \times h$ matrix, with $\ell \leq h$. The *matrix-product code* associated to A and $C_1, \ldots, C_\ell$ is denoted $C = [C_1, \ldots, C_\ell] \cdot A$, and it is the set of all matrix products $[v_1, \ldots, v_\ell] \cdot A$, where $v_i = (v_{1i}, \ldots, v_{ni})^t \in C_i$ is an $n \times 1$ column vector, for $i = 1, \ldots, \ell$. Thus, the codewords of C are $n \times h$ matrices

$$c = \begin{pmatrix} v_{11}a_{11} + \cdots + v_{1\ell}a_{\ell 1} & \cdots & v_{11}a_{1h} + \cdots + v_{1\ell}a_{\ell h} \\ \vdots & \ddots & \vdots \\ v_{n1}a_{11} + \cdots + v_{n\ell}a_{\ell 1} & \cdots & v_{n1}a_{1h} + \cdots + v_{n\ell}a_{\ell h} \end{pmatrix}.$$

Let us denote by $R_i = (a_{i,1}, \ldots, a_{i,h})$ the element of $\mathbb{F}_q^h$ given by the i-th row of A, for $1 \leq i \leq \ell$. We denote by $d_1(C_{R_i})$ the minimum distance of the code C_{R_i} generated by $\langle R_1, \ldots, R_i \rangle$ in $\mathbb{F}_q^h$. In [106] it is proven that

$$d_1(C) \geq \min\{d_1(C_1)d_1(C_{R_1}), \ldots, d_1(C_\ell)d_1(C_{R_\ell})\}, \tag{3.1}$$

where $d_1(D)$ denotes the minimum distance the code D. Moreover, in [74], the authors prove that the previous bound is sharp if $C_\ell \subset \cdots \subset C_1$. When working with MPCs, it is usual to consider the following condition, introduced in [16].

Definition 3.9. Let A be an $\ell \times h$ matrix, and let A_t be the matrix formed by the first t rows of A. For $1 \leq j_i < \cdots < j_t \leq h$, we denote by $A(j_1, \ldots, j_t)$ the $t \times t$ matrix consisting of the columns $j_1, \ldots, j_t$ of A_t. A matrix A is *non-singular by columns* (NSC) if $A(j_1, \ldots, j_t)$ is non-singular for each $1 \leq t \leq \ell$ and $1 \leq j_1 < \cdots < j_t \leq h$. In particular, an NSC matrix has full rank.

In [16] it is shown that, if A is NSC, then the codes C_{R_i} are MDS, for $1 \leq i \leq \ell$. This implies that the bound (3.1) becomes

$$d_1(C) \geq \min\{hd_1(C_1), (h-1)d_1(C_2), \ldots, (h-\ell+1)d_1(C_\ell)\} \tag{3.2}$$

for the case of an NSC matrix. One of the goals of this subsection is to generalize the bounds (3.1) and (3.2) to the case of the GHWs of C.

We start by considering a 2×2 NSC matrix A. If we denote

$$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix},$$

since A is NSC, we have $a_{1j} \neq 0$, $1 \leq j \leq 2$, and we will assume (without loss of generality) that $a_{22} \neq 0$. The following result from Paper H bounds from below the GHWs of a MPC in terms of the GHWs of sums and intersections of the constituent codes.

Theorem 3.10 [Thm. H.3.1]**.** *Let $C_1, C_2 \subset \mathbb{F}_q^n$, and let $C = [C_1, C_2] \cdot A$, with A as above. Let $1 \leq r \leq \dim C$ and consider*

$$Y = \left\{ (\alpha_1, \alpha_2) : \begin{array}{c} \max\{r - \dim(C_1 + C_2), 0\} \leq \alpha_1 \leq \min\{\dim C_2, r\} \\ \max\{r - \dim(C_1 + C_2), 0\} \leq \alpha_2 \leq \min\{\dim(C_1 \cap C_2), r\} \\ \alpha_1 + \alpha_2 \leq r \end{array} \right\}.$$

Then

$$d_r(C) \geq \min_{(\alpha_1, \alpha_2) \in Y} B_{\alpha_1, \alpha_2},$$

where

$$B_{\alpha_1,\alpha_2} = \max\{d_{r-\alpha_1}(C_1 + C_2), d_{\alpha_2}(C_1 \cap C_2)\} + \max\{d_{r-\alpha_2}(C_1 + C_2), d_{\alpha_1}(C_2)\}.$$

For the case in which the constituent codes are nested, a lower bound for the MPCs of a code with any number of constituent codes is given in Paper H, in terms of the GHWs of the constituent codes. We show next the explicit bounds we obtain for the case of two and three constituent codes, which are the most frequent cases for applications.

Corollary 3.11 [Cor. H.4.3]**.** *Let $C_2 \subset C_1 \subset \mathbb{F}_q^n$, $C = [C_1, C_2] \cdot A$, for some 2×2 NSC matrix A. Consider $1 \leq r \leq \dim C_1 + \dim C_2$, and let*

$$Y = \left\{ (\alpha_1, \alpha_2) : \begin{array}{c} \max\{r - \dim C_1, 0\} \leq \alpha_i \leq \min\{\dim C_2, r\},\ 1 \leq i \leq 2 \\ \alpha_1 + \alpha_2 \leq r \end{array} \right\}.$$

We consider

$$B_{\alpha_1,\alpha_2} = \max\{d_{r-\alpha_1}(C_1), d_{\alpha_2}(C_2)\} + \max\{d_{r-\alpha_2}(C_1), d_{\alpha_1}(C_2)\}.$$

Then

$$d_r(C) \geq \min_{(\alpha_1,\alpha_2)\in Y} B_{\alpha_1,\alpha_2}.$$

For the following result, when a subindex is greater than 3, we consider its reduction modulo 3. For instance, for $i = 2$, we have $\alpha_{i+1} + \alpha_{i+2} = \alpha_3 + \alpha_1$.

Theorem 3.12 [Thm. H.4.4]**.** *Let $C_3 \subset C_2 \subset C_1 \subset \mathbb{F}_q^n$ and $C = [C_1, C_2, C_3] \cdot A$, for some 3×3 NSC matrix A. Let $\mathbb{Z}^{3,3,1} := \mathbb{Z}^3_{\geq 0} \times \mathbb{Z}^3_{\geq 0} \times \mathbb{Z}_{\geq 0}$. Consider $1 \leq r \leq \sum_{i=1}^3 \dim C_i$, and let*

$$Y = \left\{ (\alpha, \gamma, \beta) \in \mathbb{Z}^{3,3,1} : \begin{array}{c} 0 \leq \gamma_i \leq \dim C_3,\ 1 \leq i \leq 3 \\ \max\{r - \dim C_1, \gamma_{i+1} + \gamma_{i+2}\} \leq \alpha_i,\ 1 \leq i \leq 3 \\ \alpha_{i+1} + \alpha_{i+2} - \gamma_i \leq \beta,\ 1 \leq i \leq 3 \\ \beta \leq \min\left\{ \sum_{i=1}^3 (\alpha_i - \gamma_i), \dim C_2 + \min\{\alpha_i, 1 \leq i \leq 3\}, r \right\} \end{array} \right\}.$$

For $(\alpha, \gamma, \beta) \in Y$, we consider

$$B_{\alpha,\gamma,\beta} = \sum_{i=1}^3 \max\{d_{r-\alpha_i}(C_1), d_{\beta-\alpha_i}(C_2), d_{\gamma_i}(C_3)\}.$$

Then we have

$$d_r(C) \geq \min_{(\alpha,\gamma,\beta)\in Y} B_{\alpha,\gamma,\beta}.$$

Note that Theorem 3.10 simplifies to Corollary 3.11 when assuming $C_2 \subset C_1$. Moreover, for $r = 1$, both Corollary 3.11 and Theorem 3.12 reduce to the bound (3.2). Therefore, they can be seen as a generalization of the usual bound for the minimum distance of MPCs.

In Paper H, for the nested case we also provide an upper bound for the GHWs of MPCs, which is very similar to the bound (3.1) (we recall that this bound is known to be sharp for the nested case).

Proposition 3.13 [Prop. H.5.1]. *Let $C_\ell \subset \cdots \subset C_1$, and $C = [C_1, \ldots, C_\ell] \cdot A$, where $A \subset \mathbb{F}_q^{\ell \times h}$ and has full rank. Let $1 \leq r \leq \dim C_1$ and let $1 \leq i \leq \ell$ be such that $r \leq \dim C_i$. Then*

$$d_r(C) \leq d_r(C_i) d_1(C_{R_i}).$$

As a sample of what can be obtained with our results for particular families of codes, we show the following result for Reed-Solomon codes. Here, $\mathrm{RS}(k)$ denotes a Reed-Solomon code of length $n \leq q$ and dimension k.

Theorem 3.14 [Thm. H.6.1]. *Let $1 \leq k_2 \leq k_1 \leq n \leq q$, let $A \subset \mathbb{F}_q^{2\times 2}$ be a NSC matrix, and let $\mathrm{RS}(k_1, k_2) := [\mathrm{RS}(k_1), \mathrm{RS}(k_2)] \cdot A$. For $1 \leq r \leq \dim \mathrm{RS}(k_1, k_2) = k_1 + k_2$, we have*

$$d_r(\mathrm{RS}(k_1, k_2)) = \begin{cases} 2n + r - (k_1 + k_2) & \text{if } r > \max\{k_1 - k_2, k_2\}, \\ \min\{2d_r(\mathrm{RS}(k_1)), d_r(\mathrm{RS}(k_2))\} & \text{if } r \leq \max\{k_1 - k_2, k_2\}. \end{cases}$$

4 Applications to quantum error-correction

The interest in quantum computation is rapidly growing due to the possibility of implementing algorithms with exponential speedups with respect to the classical counterparts, e.g., Shor's algorithm for finding prime factors of an integer [124]. In this setting, we are mainly interested in quantum computing and quantum communication. In both scenarios, due to noise and decoherence, the physical qudits can be subject to errors. Similarly to the classical case, one can consider *quantum error-correcting codes* (QECCs), first introduced by Shor [123], which allow us to recover the correct quantum state as long as the amount of errors does not surpass the error-correction capabilities of the QECC. Unlike the classical scenario, there are (at least) two types of errors we can consider for qudits, namely *qudit-flip* and *phase-shift errors*, which are not equally likely to occur [79, 121]. This gives rise to asymmetric QECCs, which have two minimum distances, δ_x and δ_z, meaning that they can correct up to $\lfloor (\delta_x - 1)/2 \rfloor$ qudit-flip errors and $\lfloor (\delta_z - 1)/2 \rfloor$ phase-flip errors, respectively. However, most known families QECCs are symmetric, meaning that they only consider one minimum distance $\delta = \min\{\delta_x, \delta_z\}$, that is, they are assumed to have the same error-correction capabilities for each type of error. For instance, one of the constructions we will see below only works for the symmetric case.

Focusing on the problem of constructing quantum codes, Calderbank and Shor [23], and Steane [127], independently showed how to use classical codes to construct QECCs. These constructions require self-orthogonal classical codes with respect to the Euclidean or Hermitian inner product, and the respective constructions are known as the CSS construction and the Hermitian construction, respectively. By considering entanglement between the encoder and the decoder, it is possible to construct entanglement-assisted error-correcting codes (EAQECCs) [21,48] with higher rate than usual QECCs. Even though creating and maintaining entanglement between the encoder and the decoder can be costly, the increase in rate and the fact that EAQECCs can be constructed from classical codes that are not necessarily self-orthogonal make these codes good candidates for quantum communication. Since EAQECCs are a generalization of QECCs, we state now the CSS construction in its general form for EAQECCs [48].

Theorem 4.1 (CSS construction)**.** *Let $C_i \subset \mathbb{F}_q^n$ be linear codes of dimension k_i, for $i = 1, 2$. Then, there is an asymmetric EAQECC with parameters $[[n, \kappa, \delta_z/\delta_x; c]]_q$, where*

$$c = k_1 - \dim(C_1 \cap C_2^{\perp}),\ \kappa = n - (k_1 + k_2) + c,$$
$$\delta_z = \mathrm{wt}\left(C_1^{\perp} \setminus \left(C_1^{\perp} \cap C_2\right)\right) \text{ and } \delta_x = \mathrm{wt}\left(C_2^{\perp} \setminus \left(C_2^{\perp} \cap C_1\right)\right).$$

With respect to the parameters of a quantum code, the length n is the number of physical qudits used, the dimension κ is the number of logical qudits, and the meaning of δ_z and δ_x in terms of error-correction capabilities was explained previously. Let $\delta_z^* := d_1(C_1^{\perp})$ and $\delta_x^* := d_1(C_2^{\perp})$. If $\delta_z = \delta_z^*$ and $\delta_x = \delta_x^*$, we say that the corresponding EAQECC is *pure* (or *nondegenerate*), and we say it is *impure* (or *degenerate*) if $\delta_z > \delta_z^*$ or $\delta_x > \delta_x^*$.

Regarding c, this parameter determines the minimum number required of maximally entangled pairs. Note that if we take $C_1 \subset C_2^{\perp}$, then $c = 0$. Indeed, the parameter c is determined by the dimension of the *relative hull* of C_1 with respect to C_2, which is defined in [3] as

$$\mathrm{Hull}_{C_2}(C_1) := C_1 \cap C_2^{\perp}.$$

This justifies the study of the hulls of certain families of codes, since, together with the minimum distance and dimension, they determine the parameters of the corresponding EAQECC.

For the Hermitian construction, we have to introduce first the Hermitian inner product. Let $C \subset \mathbb{F}_{q^2}^n$. The Hermitian product of two vectors $v, w \in \mathbb{F}_{q^2}^n$ is defined as

$$v \cdot_h w = \sum_{i=1}^{n} v_i w_i^q.$$

The Hermitian dual of a code $C \subset \mathbb{F}_{q^2}^n$ is defined as $C^{\perp_h} := \{v \in \mathbb{F}_{q^2}^n \mid v \cdot_h w = 0,\ \forall\, w \in C\}$. With this notation, we can introduce the Hermitian construction [48].

Theorem 4.2 (Hermitian construction)**.** *Let $C \subset \mathbb{F}_{q^2}^n$ be a linear code of dimension k and $C^{\perp_h}$ its Hermitian dual. Then, there is an EAQECC with parameters $[[n, \kappa, \delta; c]]_q$, where*

$$c = k - \dim(C \cap C^{\perp_h}),\ \kappa = n - 2k + c, \quad \text{and } \delta = d_1(C^{\perp_h} \setminus (C \cap C^{\perp_h})).$$

We note that this construction considers only the case of symmetric QECCs. Let $\delta^* = d_1(C^{\perp_h})$. In the symmetric case we say that the corresponding EAQECC is pure (or nondegenerate) if $\delta = \delta^*$, and impure (or degenerate) otherwise. Similarly to the Euclidean setting, we can define the *Hermitian hull* of C as

$$\mathrm{Hull}^H(C) = C \cap C^{\perp_h},$$

which determines the parameter c for the EAQECCs obtained from the Hermitian construction.

4.1 Quantum communication

In this section we highlight some of the results of this thesis which are better suited for quantum communication, although the codes that we obtain in this section with $c = 0$ could also be considered for fault-tolerant computation.

In Paper B, we use subfield subcodes of projective Reed-Solomon codes (mentioned in Section 2) to construct EAQECCs with both the CSS construction and the Hermitian construction. Recall the notation $\Delta_{\mathfrak{J}} = \bigcup_{\mathfrak{J}_a \subset \Delta} \mathfrak{J}_a \subset \Delta$, and we also introduce $\Delta^{\perp} := \{\alpha \in \{0, 1, \ldots, N-1\} \mid \alpha \neq N - 1 - h, h \in \Delta\}$. Also recall that $N - 1 \mid q^s - 1$. The following result shows the parameters of the asymmetric EAQECCs obtained with subfield subcodes of projective Reed-Solomon codes.

Theorem 4.3 [Thm. B.5.11]. *Let $1 \leq d_1, d_2 \leq N-1$, such that $d_i \in \mathcal{B}$, for $i = 1, 2$, and $p \mid N$. We consider $\Delta_{d_i} = \{0, 1, \ldots, d_i\}$ and we denote $\Delta'_{d_i} := \Delta_{d_i} \setminus \{d_i\}$, for $i = 1, 2$. If $((\Delta'_{d_1})_{\mathfrak{J}})^{\perp} \subset (\Delta'_{d_2})_{\mathfrak{J}}$, then we can construct an asymmetric EAQECC with parameters*

$$[[N+1, \sum_{b \in \mathcal{B}, b < d_1} n_b + \sum_{b \in \mathcal{B}, b < d_2} n_b + 2 - N, \delta_z/\delta_x; 1]]_q,$$

where $\delta_z \geq N - d_1 + 1$, $\delta_x \geq N - d_2 + 1$.

The codes from this construction are shown to outperform the ones obtained with BCH codes in [49] in Paper B.

Given $a_i \in \mathcal{A}$, we denote by a'_i the minimal element in $\mathcal{A}$ such that $\mathfrak{J}_{a'_i} = \mathfrak{J}_{-qa_i}$. Let $\Delta = \bigcup_{i=0}^{t} \mathfrak{J}_{a_i}$. We denote $\Delta^{\perp_h} := \{0, 1, \ldots, N-1\} \setminus \bigcup_{i=0}^{t} \mathfrak{J}_{a'_i}$. With the Hermitian construction, the following result is obtained using subfield subcodes of projective Reed-Solomon codes.

Theorem 4.4 [Thm. B.5.15]. *Let $\mathcal{A} = \{a_0 = 0 < a_1 < a_2 < \cdots < a_z\}$ be the set of minimal representatives of the cyclotomic sets $\mathfrak{J}_{a_i}$, $0 \leq i \leq z$, of $\{0, 1, \ldots, N-1\}$ with respect to q^2. Let $\Delta = \bigcup_{i=0}^{t-1} \mathfrak{J}_{a_i} \cup \{a_t\}$ such that $d(\Delta) < N - 1$ and $\Delta'' \subset (\Delta'')^{\perp_h}$. Then we can construct an EAQECC with parameters $[[n, \kappa, \geq \delta; c]]_q$, where $n = N + 1$, $\kappa = N + 1 - 2\left(\sum_{i=0}^{t} n_{a_i}\right) + c$, $\delta = a_t + 2$ and $c \leq 1$.*

From this construction, we find 16 new EAQECCs over $\mathbb{F}_2$, which improve the table for EAQECCs from [64].

In Paper E, we study the relative and Hermitian hull of projective Reed-Muller codes over the projective plane. Since the dual of a projective Reed-Muller code is another projective Reed-Muller code by Theorem 1.4 (if $d \not\equiv 0 \bmod q-1$), to study the relative hull we can study $\mathrm{PRM}_{d_1}(2) \cap \mathrm{PRM}_{d_2}(2)$ instead. A similar approach can be taken for the Hermitian hull, but we focus on the relative hull now for simplicity. In Paper E, we obtain the following result.

Corollary 4.5 [Cor. E.3.11]. *Let $1 \leq d_1 < d_2 \leq 2(q-1)$. Let $k_1 = \dim \mathrm{RM}_{d_1 - 1}(2)$. If $d_1 \equiv d_2 \bmod q-1$, then $\dim(\mathrm{PRM}_{d_1}(2) \cap \mathrm{PRM}_{d_2}(2)) = \dim \mathrm{PRM}_{d_1}(2)$. If $d_1 \not\equiv d_2 \bmod q-1$, then*

$$\dim(\mathrm{PRM}_{d_1}(2) \cap \mathrm{PRM}_{d_2}(2)) = \begin{cases} k_1 & \text{if } d_2 \leq q-1, \\ k_1 + \min\{d_1, d_2 - (q-1)\} & \text{if } d_1 \leq q-1 < d_2, \\ k_1 + d_2 - q + 2 & \text{if } q \leq d_1. \end{cases}$$

The techniques used to obtain this result are based on the results from Section 1. In fact, in Paper E, we obtain a set of polynomials such that its image by the evaluation map gives precisely the relative hull of the corresponding projective Reed-Muller codes. An

interesting aspect we encountered is that the relative hull (and the Hermitian hull) is not a monomial code in some cases, even though projective Reed-Muller codes are monomial codes (in the sense that they can be generated by the evaluation of monomials). This is specially relevant for the Hermitian case, and it makes the computation for that case much more involved.

By obtaining the dimension of the relative and Hermitian hull, we find all the parameters for the EAQECCs constructed with projective Reed-Muller codes over the projective plane. We obtain the following results from the CSS construction.

Theorem 4.6 [Thm. E.4.4]**.** *Let* $1 \leq d_1 \leq d_2 < 2(q-1)$*,* $d_1 + d_2 \not\equiv 0 \bmod q-1$*,* $d_1 \neq q-1 \neq d_2$*. Let* $k_1 = \dim \mathrm{RM}_{d_1-1}(2)$ *and* $k_2 = \dim \mathrm{RM}_{d_2^\perp-1}(2)$*, where* $d_2^\perp = 2(q-1) - d_2$*. Then we can construct an asymmetric EAQECC with parameters* $[[n, \kappa, \delta_z/\delta_x; c]]_q$*, where* $n = q^2+q+1$*,* $\kappa = n - (\dim \mathrm{PRM}_{d_1}(2) + \dim \mathrm{PRM}_{d_2}(2)) + c$*,* $\delta_z = \mathrm{wt}(\mathrm{PRM}_{d_2}^\perp(2))$*,* $\delta_x = \mathrm{wt}(\mathrm{PRM}_{d_1}^\perp(2))$*, and the value of* c *is the following:*

1. *If* $d_1 + d_2 < 2(q-1)$*:*

$$c = \begin{cases} d_1 + 1 - \min\{d_1, q-1-d_2\} & \text{if } d_2 < q-1, \\ d_1 + 1 & \text{if } q \leq d_2. \end{cases}$$

2. *If* $d_1 + d_2 > 2(q-1)$*:*

$$c = \begin{cases} k_1 - k_2 + d_1 + 1 & \text{if } d_1 < q-1, \\ k_1 - k_2 + q + 1 - \min\{d_2^\perp, d_1 - (q-1)\} & \text{if } q \leq d_1. \end{cases}$$

Moreover, this code is pure.

Since the use of entanglement provides both advantages (e.g., more rate) and disadvantages (it can be costly to maintain entanglement), for each application one might require different amounts of maximally entangled pairs. This gives rise to the study of families of codes with flexibility regarding the parameter c. Such flexibility can be achieved by changing the dimension of the hull via monomially equivalent codes. For this purpose, we need to introduce the following notation. The *Schur product* of two vectors $x = (x_1, \ldots, x_n)$ and $y = (y_1, \ldots, y_n)$ in $\mathbb{F}_q^n$ is defined by

$$x \star y := (x_1 y_1, \ldots, x_n y_n).$$

The *Schur product* of two codes $C_1, C_2 \subset \mathbb{F}_q^n$, denoted by $C_1 \star C_2$, is defined as the code generated by the vectors

$$\{c_1 \star c_2 : c_i \in C_i\} \subset \mathbb{F}_q^n.$$

The main result we use for the Euclidean case is the following theorem from [3].

Theorem 4.7. *For* $i = 1, 2$*, let* C_i *be* $[n, k_i]_q$ *codes with* $q > 2$*. For any* ℓ *with* $\max\{0, k_1 - k_2\} \leq \ell \leq \max \mathrm{wt}((C_1 \star C_2)^\perp) - n + k_1$*, there exists a code* $C_{1,\ell}$ *equivalent to* C_1 *such that*

$$\dim \mathrm{Hull}_{C_2}(C_{1,\ell}) = \ell.$$

In particular, if $\max \mathrm{wt}((C_1 \star C_2)^\perp) = \min\{n, 2n - k_1 - k_2\}$*,* ℓ *runs over all the possible values of* $\dim \mathrm{Hull}_{C_2}(C_1')$*, where* C_1' *is a code equivalent to* C_1*.*

For the Hermitian case, we obtain a similar result by combining the following results from [31] and [91], respectively.

Theorem 4.8. *Let $C \subset \mathbb{F}_{q^2}$ be a linear code. If there is a vector $v \in ((C \star C^q)^{\perp})_q$ with $\mathrm{wt}(v) = n$, then $\langle v \rangle \star C \subset (\langle v \rangle \star C)^{\perp_h}$, i.e., $\langle v \rangle \star C$ is self-orthogonal with respect to the Hermitian product.*

Theorem 4.9. *Let $q > 2$ and let $C \subset \mathbb{F}_{q^2}^n$ with $\dim \mathrm{Hull}_H(C) = \ell$. Then there exists a monomially equivalent code $C_{\ell'}$ with $\dim \mathrm{Hull}_H(C_{\ell'}) = \ell'$, for each $0 \leq \ell' \leq \ell$.*

In Paper F, we use these results to provide families of EAQECCs obtained with the CSS and Hermitian constructions using projective Reed-Muller codes, as we show next.

Theorem 4.10 [Thm. F.3.7]**.** *Let $1 \leq d_1 \leq d_2 < q-2$ such that $d_1 + d_2 < q-2$. Then we can construct a quantum code with parameters $[[n, \kappa + c, \delta_z/\delta_x; c]]_q$, for any $0 \leq c \leq \dim \mathrm{PRM}_{d_1}(m)$, where $n = \frac{q^{m+1}-1}{q-1}$, $\kappa = n - (\dim \mathrm{PRM}_{d_1}(m) + \dim \mathrm{PRM}_{d_2}(m))$, $\delta_z \geq \mathrm{wt}(\mathrm{PRM}_{d_2}^{\perp}(m))$ and $\delta_x \geq \mathrm{wt}(\mathrm{PRM}_{d_1}^{\perp}(m))$.*

Theorem 4.11 [Thm. F.4.6]**.** *Let $1 \leq d < q-2$. Then we can construct an EAQECC with parameters $[[n, \kappa + c, \delta; c]]_q$, for any $0 \leq c \leq \dim \mathrm{PRM}_d(q^2, m)$, where $n = \frac{q^{2(m+1)}-1}{q^2-1}$, $\kappa = n - 2(\dim \mathrm{PRM}_d(q^2, m))$ and $\delta \geq \mathrm{wt}(\mathrm{PRM}_{d^{\perp}}(q^2, m))$.*

With these constructions, we obtain many codes surpassing the quantum Gilbert-Varshamov bounds from [44, 98]. Moreover, we are also able to derive QECCs (without entanglement assistance) with subfield subcodes of projective Reed-Muller codes, using the results from Paper D.

4.2 Fault-tolerant quantum computing

For this subsection, we only consider the case $q = 2$, and we therefore write qubits instead of qudits. To achieve fault-tolerant quantum computation, we can encode the physical qubits using a QECC. By doing this, we obtain κ logical qubits which can be considered resistant to errors. One of the main problems with this approach is obtaining QECCs that implement the desired operations on the logical qubits. Particularly interesting are implementations that only involve transversal gates on the physical qubits, since they split into gates that act on individual physical qubits and they naturally mitigate the proliferation of errors. However, due to Eastin–Knill theorem [41], it is not possible to find a QECC that implements a universal gate set transversely. A common strategy to circumvent this limitation is to consider codes that implement the Clifford group transversely, and then perform magic state distillation to apply a logical non-Clifford gate, usually the T gate [20]. This is enough for implementing any gate, since adding a non-Clifford gate to the Clifford group gives a universal gate set (this is well known for the binary case, and for the general case it can be deduced from [103, Thm 6.5] and [104, Cor. 6.8.2]).

However, this requires a code implementing T transversely. In general, implementing logical non-Clifford gates is more difficult than implementing logical Clifford gates, and logical non-Clifford gates must be induced by a non-Clifford operation on the physical gates [35, 63]. Moreover, Gottesman-Knill theorem [63] also implies that quantum computation is only more powerful than classical computation when it uses gates outside the

Clifford group. The previous discussion highlights the importance of finding transversal implementations of non-Clifford gates. As we already mentioned before, the usual choice for the non-Clifford gate to be implemented via the magic state distillation protocol is the T gate due to its simplicity.

With this motivation, CSS-T were introduced in [111, 112]. These are CSS codes which support a transversal T gate, that is, applying T transversely on the physical qubits gives a logical operation over the logical qubits. This is weaker than requiring the code to implement T transversely on the logical qubits, but studying these codes gives good candidates for codes that may implement logical non-Clifford operations.

Let $C \subset \mathbb{F}_2^n$ and $S \subset \{1, \dots, n\}$. We denote by C_S (resp. C^S) the shortening (res. puncturing) of C in the coordinates indexed by the elements in S. For $x \in C$, we denote $Z(x) := \{1, \dots, n\} \setminus \mathrm{supp}(x)$, where $\mathrm{supp}(x) = \{i \mid x_i \neq 0\}$. We introduce now the definition of CSS-T codes as stated in [111].

Definition 4.12. Let $C_2 \subset C_1 \subset \mathbb{F}_2^n$. Then we say (C_1, C_2) is a *CSS-T pair* if C_2 is even-weighted and, for any $x \in C_2$, the shortening $(C_1^\perp)_{Z(x)}$ contains a self-dual code.

Note that, given a CSS-T pair (D_1, D_2), the corresponding quantum code is obtained from Theorem 4.1 by taking $C_1 = D_2$, $C_2 = D_1^\perp$.

In general, using Definition 4.12 to check if a pair of codes is a CSS-T pair is not efficient, since it would require to check a condition for every $x \in C_2$. In Paper G, we give an alternative definition by using the Schur product of codes, which we introduced previously. We also define now the *t-fold Schur product* of C with itself: $C^{\star t} := \underbrace{C \star \cdots \star C}_{t}$.

In Paper G we obtain the following result.

Theorem 4.13 [Thm. G.2.3]**.** *Let C_1 and C_2 be binary codes of length n. The following are equivalent.*

(1) *(C_1, C_2) is a CSS-T pair.*

(2) *$C_2 \subset C_1$, C_2 is even-weighted, and for any $x \in C_2$ the code $C_1^{Z(x)}$ is self-orthogonal.*

(3) *$C_2 \subset C_1 \cap (C_1^{\star 2})^\perp$.*

(4) *$C_1^\perp + C_1^{\star 2} \subset C_2^\perp$.*

Moreover, if (C_1, C_2) is a CSS-T pair then C_2 is self-orthogonal.

The alternative condition (2) was already proved in [4], but it still requires to check the self-orthogonality condition for every $x \in C_2$, whereas (3) and (4) only depend on global properties of the codes C_1 and C_2. With these alternative conditions, we define the partially ordered set (poset) of CSS-T pairs. In Paper G, we study this poset and, as a consequence, we obtain the following propagation rule for CSS-T pairs.

Corollary 4.14 [Cor. G.3.9]**.** *Let (C_1, C_2) be a CSS-T pair such that the associated $[[n, k, d]]$ CSS-T code is nondegenerate. For any $y \in C_2^\perp \cap (C_1 \star C_2)^\perp$ and $y \notin C_1$, the pair $(C_1 + \langle y \rangle, C_2)$ is a nondegenerate CSS-T pair with parameters*

$$[[n, k+1, d]].$$

Using our characterization of CSS-T pairs, we determine the CSS-T pairs formed by cyclic (and extended cyclic) codes. Take an integer $s > 1$ and consider the field extension $\mathbb{F}_{2^s}/\mathbb{F}_2$. We set n with $n \mid 2^s - 1$. Let $\beta \in \mathbb{F}_{2^s}$ be a primitive n-th root of unity. For the set $\mathbb{Z}/n\mathbb{Z}$, we will consider the representatives between 1 and n, i.e., $\mathbb{Z}/n\mathbb{Z} = \{1, 2, \ldots, n\}$.

Definition 4.15. Let $g \in \mathbb{F}_2[x]$ such that g divides $x^n - 1$. The *defining set* is given by $J := \{j \in \mathbb{Z}/n\mathbb{Z} : g(\beta^j) = 0\}$, and the *generating set* by $I := \{i \in \mathbb{Z}/n\mathbb{Z} : g(\beta^i) \neq 0\}$.

We denote by $C(I)$ the cyclic code generated by g. Note that cyclic codes can be regarded as subfield subcodes of evaluation codes [13], and therefore some of the ideas showed in Section 2 about cyclotomic sets and traces can be applied here. In Paper G, we obtain the following characterization for the CSS-T pairs arising from cyclic codes.

Theorem 4.16 [Thm. G.4.8]**.** *Let $I_1, I_2 \subset \mathbb{Z}/n\mathbb{Z}$ be cyclotomic cosets. Then $(C(I_1), C(I_2))$ is a CSS-T pair if and only if:*

(1) $I_2 \subset I_1$ *and*

(2) $n \notin (I_1 + I_1 + I_2)$.

An analogous result holds for extended cyclic codes. The resulting CSS-T codes have better parameters than the CSS-T codes in the current literature, namely the CSS-T pairs arising from Reed-Muller codes [4], and triorthogonal codes [19, 70, 105]. Note that triorthogonal codes not only support the transversal T gate, but they also induce the logical T gate. Since this is a stronger condition than being CSS-T, it is natural that we obtain better parameters.

Part II

Publications

Paper A

Saturation and vanishing ideals

Philippe Gimenez, Diego Ruano, Rodrigo San-José

Abstract

We consider an homogeneous ideal I in the polynomial ring $S = K[x_1, \ldots, x_m]$ over a finite field $K = \mathbb{F}_q$ and the finite set of projective rational points $\mathbb{X}$ that it defines in the projective space $\mathbb{P}^{m-1}$. We concern ourselves with the problem of computing the vanishing ideal $I(\mathbb{X})$. This is usually done by adding the equations of the projective space $I(\mathbb{P}^{m-1})$ to I and computing the radical. We give an alternative and more efficient way using the saturation with respect to the homogeneous maximal ideal.

Keywords: Projective codes, evaluation codes, vanishing ideal, saturation, radical.
MSC: 13P25, 13M10, 94B27.
DOI: 10.1007/s40863-022-00330-y
Reference: P. Gimenez, D. Ruano, R. San-José. Saturation and vanishing ideals. São Paulo J. Math. Sci., 17, 147-155 (2023).
Affiliation: Philippe Gimenez, Diego Ruano, Rodrigo San-José: IMUVA-Mathematics Research Institute, Universidad de Valladolid.

A.1 Introduction

The aim of this paper is to compute the vanishing ideal of a finite set of points in the projective space. The motivation comes from Coding Theory, in which some projective codes are defined using these type of ideals. In the affine case, the computation of the vanishing ideal of a finite set of points is straightforward, but the projective case poses some additional problems. It is known that the vanishing ideal can be obtained computing the radical of a certain ideal, and we show that it can also be obtained computing the saturation with respect to the homogeneous maximal ideal, which is more efficient.

Let $K = \mathbb{F}_q$ be a finite field, and let $S = K[x_1, \ldots, x_m]$ be the polynomial ring with standard grading. Let $I \subset S$ be an ideal. We denote by $X = V_{\mathbb{F}_q}(I) = \{P_1, \ldots, P_n\} \subset \mathbb{A}^m$ the finite set of rational points in which all the polynomials of I vanish. Then we can consider the vanishing ideal of X, $I(X)$. With this notation we define the following evaluation map:

$$\mathrm{ev}_X : S/I(X) \to \mathbb{F}_q^n, \;\; f + I(X) \mapsto (f(P_1), \ldots, f(P_n)) \,.$$

By the definition of $I(X)$, this evaluation map is an isomorphism of $\mathbb{F}_q$-vector spaces. If we consider L a vector subspace of $S/I(X)$, we can define the *affine variety code* $C(I, L)$ as the image of L under the evaluation map ev_X. That is:

$$C(I, L) = \mathrm{ev}_X(L) = \{\mathrm{ev}_X(f + I(X)) \mid f + I(X) \in L\}.$$

In the light of this definition one may wonder how to compute the ideal $I(X)$. In this affine setting, the answer is quite straightforward. The ideal $I_q = I + \langle x_1^q - x_1, \ldots, x_m^q - x_m \rangle$ satisfies

$$V_{\overline{\mathbb{F}_q}}(I_q) = V_{\mathbb{F}_q}(I_q) = V_{\mathbb{F}_q}(I) = V_{\mathbb{F}_q}(I(X)) = X.$$

By Seidenberg's Lemma [13, Prop. 3.7.15], I_q is radical. Hence, in this case $I_q = I(X)$ and we obtain the vanishing ideal directly.

Following a similar idea, one can consider evaluation codes over the projective space $\mathbb{P}^{m-1}$. Let $I \subset S$ be an homogeneous ideal. Again, we consider $\mathbb{X} = V_{\mathbb{P}^{m-1}}(I) = \{[P_1], \ldots, [P_n]\} \subset \mathbb{P}^{m-1}$ the finite set of projective points defined by I with representatives P_i. Denoting the vanishing ideal of $\mathbb{X}$ by $I(\mathbb{X})$, we can define the following K-linear map for each degree d:

$$\mathrm{ev}_d : S_d \to K^n, \;\; f \mapsto \left(\frac{f(P_1)}{f_1(P_1)}, \ldots, \frac{f(P_n)}{f_n(P_n)} \right),$$

where $f_i \in S_d$ are fixed homogeneous polynomials verifying $f_i(P_i) \neq 0$. Then the image of S_d under ev_d, denoted by $C_{\mathbb{X}}(d)$, is called a *projective Reed-Muller type code* of degree d on $\mathbb{X}$. By definition, $I(\mathbb{X})_d = \ker \mathrm{ev}_d$. Thus, $S_d/I(\mathbb{X})_d \cong C_{\mathbb{X}}(d)$. It can easily be checked that the basic parameters of the code (length, dimension and minimum distance) do not depend on the choice of the polynomials f_i. These codes have been studied in various contexts [3–5, 9, 17].

In order to compute $I(\mathbb{X})$, as in the affine case, a natural idea would be to add the equations of the projective space to the ideal I, and check whether the resulting ideal is radical. These equations correspond to the generators of the vanishing ideal of the set of all points in $\mathbb{P}^{m-1}$ [15]:

$$I(\mathbb{P}^{m-1}) = \langle \{x_i^q x_j - x_i x_j^q, 1 \leq i < j \leq m\} \rangle.$$

We can define $I_q = I + I(\mathbb{P}^{m-1})$ and, as before, if this ideal were radical, then it would be equal to $I(\mathbb{X})$. However, this ideal is not radical in general. In fact, we have observed that this ideal is radical only in very specific cases. In general, computing the radical may be computationally intensive. Thus, it is an interesting problem to find an easier way to compute $I(\mathbb{X})$.

In Theorem A.2.10, we prove that we can compute the vanishing ideal $I(\mathbb{X})$ using the saturation with respect to the homogeneous maximal ideal:

$$I(\mathbb{X}) = (I + I(\mathbb{P}^{m-1})) : \mathfrak{m}^{\infty}).$$

We then ask ourselves if there are many cases in which there is no need to use the saturation, i.e., $I + I(\mathbb{P}^{m-1}) = I(\mathbb{X})$. The answer is that this rarely happens, because it is equivalent to the question of whether I_q is radical or not. Following this direction, in Proposition A.2.15, we show that there are finite sets of points $\mathbb{X} \subset \mathbb{P}^{m-1}$ such that there is no ideal $I \subset S$, besides $I(\mathbb{X})$, such that $I + I(\mathbb{P}^{m-1}) = I(\mathbb{X})$.

A.2 Main result

Before providing the main result, we recall some well known results. The first one is often referred as *additivity of the degree*.

Proposition A.2.1 [11, Lem. 5.3.11]**.** *Let $I \subset S$ be an homogeneous ideal and let $I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_m$ be its irredundant primary decomposition. Then*

$$\deg(S/I) = \sum_{\mathrm{ht}(\mathfrak{q}_i)=\mathrm{ht}(I)} \deg(S/\mathfrak{q}_i).$$

The vanishing ideal of a finite set of points satisfies many properties. We list some of them below.

Lemma A.2.2 [14, Cor. 6.3.19]**.** *Let $[\alpha] \in \mathbb{P}^{m-1}$, with $\alpha = (\alpha_1, \ldots, \alpha_m)$, and let $I_{[\alpha]} = I(\{[\alpha]\})$ its vanishing ideal. Then*

$$I_{[\alpha]} = (\{\alpha_i x_j - \alpha_j x_i \mid 0 \leq i < j \leq m\}).$$

Remark A.2.3. In the previous lemma, at least one $\alpha_k \neq 0$ for some k. Hence, we can express $I_{[\alpha]}$ in the following way:

$$I_{[\alpha]} = (\{x_i - \frac{\alpha_i}{\alpha_k} x_k \mid i = 1, \ldots, n, i \neq k\}).$$

Corollary A.2.4. *The ideal $I_{[\alpha]}$ is prime, $\deg(S/I_{[\alpha]}) = 1$ and $\mathrm{ht}(I_{[\alpha]}) = m - 1$.*

Proof. All properties follow from the fact that $S/I_{[\alpha]} \cong K[x_k]$ for some k, which is obvious from the previous remark. □

Remark A.2.5. If we have a finite subset $\mathbb{X} \subset \mathbb{P}^{m-1}$, then

$$I(\mathbb{X}) = \bigcap_{[\beta] \in \mathbb{X}} I_{[\beta]}.$$

Taking into account that each $I_{[\beta]}$ is prime, the previous expression is an irredundant primary decomposition of $I(\mathbb{X})$.

Corollary A.2.6. *Let $\mathbb{X} \subset \mathbb{P}^{m-1}$ be a finite subset. Then $\deg(S/I(\mathbb{X})) = |\mathbb{X}|$, $\mathrm{ht}(I(\mathbb{X})) = m-1$, and $S/I(\mathbb{X})$ is Cohen-Macaulay.*

Proof. The first property follows from Proposition A.2.1 and the previous remark. The second one follows from Corollary A.2.4 and the previous remark. The last one is deduced from the fact that $\mathrm{depth}(I(\mathbb{X})) = 0$ if and only if $I(\mathbb{X})$ has an $\mathfrak{m}$-primary component, which is not the case because of the previous remark, and the fact that $\dim S/I(\mathbb{X}) = 1$. □

The following lemma is interesting because it relates the number of common zeros of a set of polynomials to the degree of a certain ideal, which gives a relation between Coding Theory and Commutative Algebra.

Lemma A.2.7 [9, Lem. 3.4]**.** *Let $\mathbb{X}$ be a finite subset of $\mathbb{P}^{m-1}$ over a field K, and let $I(\mathbb{X}) \subset S$ be its vanishing ideal. If $F = \{f_1, \ldots, f_r\}$ is a set of homogeneous polynomials of $S \setminus \{0\}$, then the number of points of $V_{\mathbb{X}}(F)$ (common zeroes of F which are in $\mathbb{X}$) is given by*

$$|V_{\mathbb{X}}(F)| = \begin{cases} \deg(S/(I(\mathbb{X}), F)) & \text{if } (I(\mathbb{X}) : (F)) \neq I(\mathbb{X}), \\ 0 & \text{if } (I(\mathbb{X}) : (F)) = I(\mathbb{X}). \end{cases}$$

Lemma A.2.8 [8, Lem. 8]**.** *Let $I \subset J \subset S$ be unmixed homogeneous ideals with the same height. If $\deg(S/I) = \deg(S/J)$, then $I = J$.*

The computation of the vanishing ideal only makes sense when $\mathbb{X} = V_{\mathbb{P}^{m-1}}(I) \neq \emptyset$. One can get $\mathbb{X} = \emptyset$ in several ways, for example, if I is 0-dimensional, or if it has positive dimension but no common zero of the homogeneous polynomials in I is in $\mathbb{P}^{m-1}$ for the corresponding field $\mathbb{F}_q$. The following lemma gives an algebraic characterization of this property.

Lemma A.2.9. *Let $I \subset S$ be an homogeneous ideal. Then $\mathbb{X} = V_{\mathbb{P}^{m-1}}(I) = \emptyset$ if and only if $(I(\mathbb{P}^{m-1}) : I) = I(\mathbb{P}^{m-1})$.*

Proof. We have $\mathbb{X} = V_{\mathbb{P}^{m-1}}(I) = \emptyset$ if and only if $I \not\subset I_{[P]}$ for any $[P] \in \mathbb{P}^{m-1}$. We also have that $(I_{[P]} : I) = I_{[P]}$ if and only if $I \not\subset I_{[P]}$ because $I_{[P]}$ is prime. Therefore, $I \not\subset I_{[P]}$ for any $[P] \in \mathbb{P}^{m-1}$ if and only if $(I(\mathbb{P}^{m-1}) : I) = I(\mathbb{P}^{m-1})$ because

$$(I(\mathbb{P}^{m-1}) : I) = \bigcap_{[P] \in \mathbb{P}^{m-1}} (I_{[P]} : I),$$

so the result is proved. □

The natural way of computing $I(\mathbb{X})$ from the point of view of Coding Theory is by taking the radical of $I_q = I + I(\mathbb{P}^{m-1})$, similarly to what is done in the affine case (although in that case, I_q is always radical). For this, we have to prove that

$$I(\mathbb{X}) = \sqrt{I + I(\mathbb{P}^{m-1})}.$$

This can be seen as an application of Hilbert's Nullstellensatz in the algebraic closure of $\mathbb{F}_q$, or can be proved directly as in [12, Thm. 3.13]. Inspired by the proof of the latter, the following theorem shows a way to compute $I(\mathbb{X})$ using the saturation with respect to the homogeneous maximal ideal. This is also a natural way to compute $I(\mathbb{X})$ from the

point of view of Commutative Algebra, because we are getting rid of the 0-dimensional components, which are meaningless in this projective setting. Note that saturation with respect to a specific element has been used for similar purposes in [16, Cor. 4.4] for certain projective binomial varieties.

Theorem A.2.10. *Let I be an homogeneous ideal such that $(I(\mathbb{P}^{m-1}) : I) \neq I(\mathbb{P}^{m-1})$. Let $\mathbb{X} = V_{\mathbb{P}^{m-1}}(I)$ and $\mathfrak{m} = (x_1, \ldots, x_m)$ the homogeneous maximal ideal. Then*

$$I(\mathbb{X}) = (I + I(\mathbb{P}^{m-1})) : \mathfrak{m}^{\infty}.$$

Proof. Again we denote $I_q = I + I(\mathbb{P}^{m-1})$ and we are going to prove first that $\deg(S/I_q) = \deg(S/I(\mathbb{X}))$. We can apply Lemma A.2.7 to $\mathbb{X} = \mathbb{P}^{m-1}$ and a set of generators F of I. We obtain:

$$|\mathbb{X}| = |V_{\mathbb{P}^{m-1}}(I)| = \deg(S/I_q),$$

and because $|\mathbb{X}| = \deg(S/I(\mathbb{X}))$ holds by Corollary A.2.6, we get the equality $\deg(S/I_q) = \deg(S/I(\mathbb{X}))$.

On the other hand, we have that $\sqrt{I_q} = I(\mathbb{X})$. Thus, $\dim(S/I_q) = 1$ and the primary decomposition is

$$I_q = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_l \cap Q,$$

where $\dim(S/\mathfrak{q}_i) = 1$, $1 \leq i \leq l$, and Q is the whole ring S if I_q is equidimensional, and an $\mathfrak{m}$-primary ideal otherwise. If we consider the irredundant primary decomposition $I(\mathbb{X}) = \bigcap_{[P_i] \in \mathbb{X}} I_{[P_i]}$, with $|\mathbb{X}| = n$, then we get the equality

$$I_{[P_1]} \cap \cdots \cap I_{[P_n]} = \sqrt{\mathfrak{q}_1} \cap \cdots \cap \sqrt{\mathfrak{q}_l} \cap \sqrt{Q} = \sqrt{\mathfrak{q}_1} \cap \cdots \cap \sqrt{\mathfrak{q}_l}.$$

Reordering if necessary, we have that $I_{[P_i]} = \sqrt{\mathfrak{q}_i}$, $1 \leq i \leq n$ and $l \geq n$. Taking into account that $\deg(S/I_q) = \deg(S/I(\mathbb{X}))$, the additivity of the degree A.2.1 and $\deg(S/I_{[P_i]}) = 1$ for all i, we get

$$|\mathbb{X}| = n = \sum_{i=1}^{n} \deg(S/I_{[P_i]}) = \sum_{i=1}^{l} \deg(S/\mathfrak{q}_i) \geq l.$$

As observed before, $l \geq n$, which, together with the previous inequality, gives $l = n$. Moreover, we deduce $\deg(S/\mathfrak{q}_i) = 1$ for all i, $1 \leq i \leq n$. Therefore, using that $I_{[P_i]} = \sqrt{\mathfrak{q}_i} \supset \mathfrak{q}_i$, $1 \leq i \leq n$ and Lemma A.2.8 we have that $\mathfrak{q}_i = I_{[P_i]}$, $1 \leq i \leq n$. Finally, we observe that

$$(I_q : \mathfrak{m}^{\infty}) = (I_{[P_1]} : \mathfrak{m}^{\infty}) \cap \cdots \cap (I_{[P_n]} : \mathfrak{m}^{\infty}) \cap (Q : \mathfrak{m}^{\infty}) = I_{[P_1]} \cap \cdots \cap I_{[P_n]} = I(\mathbb{X}),$$

and the result holds. □

Theorem A.2.10 gives a more efficient way of computing the vanishing ideal $I(\mathbb{X})$ than the usual way using the radical. For the computations we needed to choose between the different computer algebra systems, the main ones for Commutative Algebra are CoCoA [1], Singular [6] and Macaulay2 [10]. We chose Macaulay2 for the examples on this occasion. We have used a computer with 512GB of RAM and an AMD EPYC 7F52 processor.

Example A.2.11. We consider the 3-dimensional rational normal scroll defined by the equations given by the 2×2 minors of the following matrix:

$$M = \begin{pmatrix} x_0 & x_1 & x_2 & x_3 & x_4 & y_0 & y_1 & y_2 & y_3 & y_4 & z_0 & z_1 & z_2 & z_3 & z_4 \\ x_1 & x_2 & x_3 & x_4 & x_5 & y_1 & y_2 & y_3 & y_4 & y_5 & z_1 & z_2 & z_3 & z_4 & z_5 \end{pmatrix},$$

and let I be the homogeneous ideal defined by these equations. The number of rational points of this variety on $\mathbb{F}_q$ is $(q^2+q+1)(q+1)$ [4, Cor. 2.3]. We first consider the case with $q = 9$. In this situation, $|\mathbb{X}| = 910$, and the computation of the saturation with Macaulay2 [10] takes 3.65 seconds. However, the computation of the radical of I_q takes 1108.15 seconds, which shows the big difference in efficiency between the two methods.

If we consider the case $q = 11$ instead, we have $|\mathbb{X}| = 1596$. The saturation takes 5.08 seconds, and Macaulay2 [10] is not able to compute the radical of the ideal.

For this example, we have also considered Magma [2], which seems to have a well-optimized algorithm to compute the radical over fields of positive characteristic. Although the efficiency gap is reduced, the saturation is still more efficient than computing the radical.

Remark A.2.12. It is always possible to obtain the vanishing ideal using the saturation with respect to a single polynomial. Because of prime avoidance [7, Lemma 3.3] there is a homogeneous polynomial $f \in S$ such that $f \notin I_{[P_i]}$, for every $[P_i] \in \mathbb{X}$, i.e., f does not vanish at any of the points of $\mathbb{X}$. Then, following the proof of Theorem A.2.10, we get

$$(I_q : f^\infty) = \left(\bigcap_{[P_i] \in \mathbb{X}} (I_{[P_i]} : f^\infty) \right) \cap (Q : f^\infty) = \bigcap_{[P_i] \in \mathbb{X}} I_{[P_i]} = I(\mathbb{X}).$$

The problem is that finding such a polynomial f may not be easy. However, in some specific examples, such as the following one, it can be done.

Example A.2.13. Let I be the homogeneous ideal of the rational normal curve defined by the equations given by the 2×2 minors of the matrix

$$N = \begin{pmatrix} x_0 & x_1 & x_2 & x_3 & x_4 \\ x_1 & x_2 & x_3 & x_4 & x_5 \end{pmatrix}.$$

We work over the field $\mathbb{F}_9$, and we consider the polynomial $f = x_0 - x_4 - x_5$. If we define $I_9 = I + I(\mathbb{P}^5)$, then it is easy to check with Macaulay2 [10] that $(I_9 : f^\infty) = (I_9 : \mathfrak{m}^\infty) = I(\mathbb{X})$, and that f does not vanish at any of the points in $\mathbb{X}$, i.e., $(I(\mathbb{X}) : f) = I(\mathbb{X})$.

Having seen how to compute the vanishing ideal $I(\mathbb{X})$, one may wonder if there are many cases in which I_q is saturated. If that were the case, we would not need to compute the saturation and we would get the vanishing ideal directly. An equivalent question would be to ask when the equality $I + I(\mathbb{P}^{m-1}) = I(\mathbb{X})$ holds. It is easy to see that if one takes $I = I(\mathbb{X})$, the vanishing ideal of a finite set of points $\mathbb{X} \subset \mathbb{P}^{m-1}$, then $I(\mathbb{X}) + I(\mathbb{P}^{m-1}) = I(\mathbb{X})$. Another trivial example would be to take an ideal I with $V_{\mathbb{P}^{m-1}}(I) = \mathbb{P}^{m-1}$. We can also find some nontrivial examples, like the following one.

Example A.2.14. Let $K = \mathbb{F}_4$ and $\mathbb{X} = [\mathbb{F}_2 \times \mathbb{F}_2 \times \mathbb{F}_4] \subset \mathbb{P}^2$. We can compute the vanishing ideal $I(\mathbb{X})$ directly (intersecting the vanishing ideals of the points in $\mathbb{X}$), but we can also use [3, Prop. 2.11]. In any case, we obtain

$$I(\mathbb{X}) = (x_1x_2^2 + x_1^2x_2, x_1x_3^4 + x_1^4x_3, x_2x_3^4 + x_2^4x_3).$$

We consider the ideal I, obtained by replacing the primary component (x_1, x_2) of $I(\mathbb{X})$ by $(x_1, x_2)^2$. Clearly $\mathbb{X} = V_{\mathbb{P}^2}(I)$. In this situation, it turns out that $I + I(\mathbb{P}^2) = I(\mathbb{X})$. This is easy to check by looking at the generators of these ideals:

$$\begin{aligned} I(\mathbb{P}^2) &= (x_1x_2^4 + x_1^4x_2, x_1x_3^4 + x_1^4x_3, x_2x_3^4 + x_2^4x_3), \\ I &= (x_1x_2^2 + x_1^2x_2, x_1(x_1x_3^4 + x_1^4x_3), x_2(x_1x_3^4 + x_1^4x_3), x_2(x_2x_3^4 + x_2^4x_3)), \\ I(\mathbb{X}) &= (x_1x_2^2 + x_1^2x_2, x_1x_3^4 + x_1^4x_3, x_2x_3^4 + x_2^4x_3). \end{aligned}$$

Similar examples can be constructed by considering $\mathbb{X} = \mathbb{F}_{p^l} \times \mathbb{F}_{p^l} \times \mathbb{F}_{p^{l'}}$, with $l \mid l'$, and increasing the multiplicity of the component (x_1, x_2).

Even though we can construct several nontrivial examples, one can observe that in order to do so we have not strayed away too much from $I(\mathbb{P}^{m-1})$ and $I(\mathbb{X})$ (we have just used an ideal $I(\mathbb{X})$ that shares some generators with $I(\mathbb{P}^{m-1})$ and modified it a little). In fact, in most cases we have encountered, I_q was not saturated. The next result shows that there are some finite sets of points $\mathbb{X}$ such that there are no nontrivial homogeneous ideals I with $V_{\mathbb{P}^{m-1}}(I) = \mathbb{X}$ verifying $I + I(\mathbb{P}^{m-1}) = I(\mathbb{X})$.

Proposition A.2.15. *Let $\mathbb{X} \subset \mathbb{P}^m$ be a finite set of points such that the degree of the elements of a minimal generating set of $I(\mathbb{X})$ is lower than $q+1$. Then $I + I(\mathbb{P}^m) = I(\mathbb{X})$ if and only if $I = I(\mathbb{X})$.*

Proof. Let I be an homogeneous ideal verifying $I + I(\mathbb{P}^m) = I(\mathbb{X})$. Obviously, $I \subset I(\mathbb{X})$, and we have to prove the other inclusion. The degree of the minimal generators of $I(\mathbb{P}^m)$ is $q + 1$. Therefore, the minimal generators of $I(\mathbb{X})$, of degree lower than $q + 1$, must all be in I, which proves the result. □

Example A.2.16. Let $K = \mathbb{F}_4$, and let $\mathbb{X} = [\mathbb{F}_2 \times \mathbb{F}_2 \times \mathbb{F}_2] \subset \mathbb{P}^2$. The vanishing ideal $I(\mathbb{X})$ is the same as $I(\mathbb{P}^2)$ in $\mathbb{F}_2$. Therefore, we have

$$I(\mathbb{X}) = (x_1^2x_2 - x_1x_2^2, x_1^2x_3 - x_1x_3^2, x_2^2x_3 - x_2x_3^2).$$

The generators of $I(\mathbb{X})$ are of degree $3 < 5 = q+1$. Consequently, we can use Proposition A.2.15 to assert that there is no homogeneous ideal I, besides $I(\mathbb{X})$, such that $I + I(\mathbb{P}^2) = I(\mathbb{X})$.

In the proof of A.2.10 we showed that $\deg(S/I_q) = \deg(S/I(\mathbb{X}))$. Also, taking into account that $\dim(S/I(\mathbb{X})) = 1$ and that $\sqrt{I_q} = I(\mathbb{X})$, we get $\mathrm{ht}(I_q) = \mathrm{ht}(I(\mathbb{X}))$. As we have said, in most cases, $I_q \neq I(\mathbb{X})$. Consequently, we would have $I_q \subsetneq I(\mathbb{X})$, but $\deg(S/I_q) = \deg(S/I(\mathbb{X}))$. The following example illustrates this fact, which seems to contradict [5, Lem. 2.10 (b)].

Example A.2.17. We consider again the set $\mathbb{X} = [\mathbb{F}_2 \times \mathbb{F}_2 \times \mathbb{F}_4] \subset \mathbb{P}^2$ from example A.2.14. We can replace the primary component (x_1, x_3) by $(x_1, x_3)^2$ in the primary decomposition of $I(\mathbb{X})$, which gives the following ideal:

$$I = I(\mathbb{X}) \cap (x_1, x_3)^2 = (x_1(x_1x_2^2 + x_1^2x_2), x_1(x_1x_2x_3 + x_2^2x_3), x_1x_3^4 + x_1^4x_3, x_3(x_2x_3^4 + x_2^4x_3)).$$

We can define $I_4 = I + I(\mathbb{P}^2)$ and it is easy to check with Macaulay2 [10] that $I_4 \subsetneq I(\mathbb{X})$, $\mathrm{ht}(I_4) = \mathrm{ht}(I(\mathbb{X})) = 2$ and $\deg(S/I_4) = \deg(S/I(\mathbb{X}))$, which contradicts [5, Lem. 2.10 (b)]. Increasing the multiplicity of any primary component of $I(\mathbb{X})$, besides (x_1, x_2), we get more examples of ideals I such that $I_4 = I + I(\mathbb{P}^2)$ is not saturated and has the same degree and height as $I(\mathbb{X})$. Note that this does not contradict Lemma A.2.8 since I_4 is not unmixed.

Bibliography

[1] J. Abbott, A. M. Bigatti, and L. Robbiano. CoCoA: a system for doing Computations in Commutative Algebra. Available at `http://cocoa.dima.unige.it`.

[2] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[3] C. Carvalho, V. G. L. Neumann, and H. H. López. Projective nested cartesian codes. *Bull. Braz. Math. Soc. (N.S.)*, 48(2):283–302, 2017.

[4] C. Carvalho, X. Ramírez-Mondragón, V. G. L. Neumann, and H. Tapia-Recillas. Projective Reed-Muller type codes on higher dimensional scrolls. *Des. Codes Cryptogr.*, 87(9):2027–2042, 2019.

[5] S. M. Cooper, A. Seceleanu, Ş. O. Tohăneanu, M. V. Pinto, and R. H. Villarreal. Generalized minimum distance functions and algebraic invariants of Geramita ideals. *Adv. in Appl. Math.*, 112:101940, 34, 2020.

[6] W. Decker, G.-M. Greuel, G. Pfister, and H. Schönemann. SINGULAR 4-4-0 — A computer algebra system for polynomial computations. `http://www.singular.uni-kl.de`, 2024.

[7] D. Eisenbud. *Commutative algebra*, volume 150 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1995. With a view toward algebraic geometry.

[8] B. Engheta. On the projective dimension and the unmixed part of three cubics. *J. Algebra*, 316(2):715–734, 2007.

[9] M. González-Sarabia, J. Martínez-Bernal, R. H. Villarreal, and C. E. Vivares. Generalized minimum distance functions. *J. Algebraic Combin.*, 50(3):317–346, 2019.

[10] D. R. Grayson and M. E. Stillman. Macaulay2, a software system for research in algebraic geometry.

[11] G.-M. Greuel and G. Pfister. *A* **Singular** *introduction to commutative algebra*. Springer, Berlin, extended edition, 2008. With contributions by Olaf Bachmann, Christoph Lossen and Hans Schönemann.

[12] D. Jaramillo, M. Vaz Pinto, and R. H. Villarreal. Evaluation codes and their basic parameters. *Des. Codes Cryptogr.*, 89(2):269–300, 2021.

[13] M. Kreuzer and L. Robbiano. *Computational commutative algebra. 1*. Springer-Verlag, Berlin, 2000.

[14] M. Kreuzer and L. Robbiano. *Computational commutative algebra. 2*. Springer-Verlag, Berlin, 2005.

[15] D.-J. Mercier and R. Rolland. Polynômes homogènes qui s'annulent sur l'espace projectif $\mathrm{P}^m(\mathbf{F}_q)$. *J. Pure Appl. Algebra*, 124(1-3):227–240, 1998.

[16] C. Rentería-Márquez, A. Simis, and R. H. Villarreal. Algebraic methods for parameterized codes and invariants of vanishing ideals over finite fields. *Finite Fields Appl.*, 17(1):81–104, 2011.

[17] A. B. Sørensen. Projective Reed-Muller codes. *IEEE Trans. Inform. Theory*, 37(6):1567–1576, 1991.

Paper B

Entanglement-assisted quantum error-correcting codes from subfield subcodes of projective Reed-Solomon codes

Philippe Gimenez, Diego Ruano, Rodrigo San-José

Abstract

We study the subfield subcodes of projective Reed-Solomon codes and their duals: we provide bases for these codes and estimate their parameters. With this knowledge, we can construct symmetric and asymmetric entanglement-assisted quantum error-correcting codes, which in many cases have new or better parameters than the ones available in the literature.

Keywords: Asymmetric quantum codes, EAQECC, evaluation codes, linear codes, projective Reed-Solomon codes, subfield subcodes, trace.

MSC: 81P70, 94B05, 13P25.

DOI: 10.1007/s40314-023-02506-4

Reference: P. Gimenez, D. Ruano, R. San-José. Entanglement-assisted quantum error-correcting codes from subfield subcodes of projective Reed-Solomon codes. Comp. Appl. Math. 42, 363 (2023).

Affiliation: Philippe Gimenez, Diego Ruano, Rodrigo San-José: IMUVA-Mathematics Research Institute, Universidad de Valladolid.

B.1 Introduction

The subfield subcode of a linear code $C \subset \mathbb{F}_{q^s}^n$, with $s \geq 1$, is the linear code $C \cap \mathbb{F}_q^n$. Considering subfield subcodes is a standard technique for constructing long linear codes over a small finite field. For instance, BCH codes are obtained in this way. They can be regarded as subfield subcodes of Reed-Solomon codes and their duals [2]. In this work, we study subfield subcodes of projective Reed-Solomon codes.

Reed-Solomon codes are constructed by evaluating one-variable polynomials at points of the affine line. They have optimal parameters, although they cannot be defined over a small finite field. Projective Reed-Solomon codes are constructed by evaluating two-variable homogeneous polynomials at points of the projective line. When one evaluates at all the points they are commonly called doubly extended Reed-Solomon codes. Subfield subcodes of projective Reed-Solomon codes, when one evaluates at all the points of the projective line, were studied in [3].

In this work we consider a more general setting: we may evaluate at fewer points to define a projective Reed-Solomon code and then compute its subfield subcode. We provide bases for both the subfield subcodes of projective Reed-Solomon codes and their duals and, thus, a formula for their dimension. For the dual code, we use Delsarte's Theorem B.4.1, for which we need to study first the metric structure of the codes we are considering. We also study the vanishing ideal of the points in which we evaluate, which allows us to discuss linear independence between the traces that arise when using Delsarte's Theorem. Moreover, we estimate the minimum distance for both primary and dual codes. For the primary code we simply use the bound given by the projective Reed-Solomon code, and for the dual one we use a BCH-type bound.

Reed-Solomon and BCH codes have been extensively used to construct quantum codes using the CSS construction, see for instance [4, 19, 27]. It is therefore natural to consider subfield subcodes of projective Reed-Solomon for constructing quantum codes.

The construction of quantum computers has important consequences because of their computing capabilities. Despite the fact that quantum mechanical systems are sensitive to disturbances and arbitrary quantum states cannot be replicated, error correction is possible. Quantum error-correcting codes are designed for protecting quantum information from quantum noise and particularly decoherence. An important class of quantum error-correcting codes are stabilizer codes; they can be derived from classical ones by using self-orthogonal codes for the symplectic product [7]. One can also consider the Euclidean and the Hermitian inner product, and we will call the resulting quantum error-correcting codes QECCs. Entanglement-assisted quantum error-correcting codes (EAQECCs) constitute an extension of quantum codes. EAQECCs make use of pre-existing entanglement between transmitter and receiver to correct more errors [6, 15]. One virtue of this class of codes is that one can get a quantum code from any linear code without any assumption on dual containment. The main additional task for EAQECCs is to give formulae to obtain the optimal number c of maximally entangled pairs of qudits needed.

Moreover, both for QECCs and EAQECCs one can consider the asymmetric case [16, 25, 33]. Asymmetric quantum codes have a different error-correction capability for phase-shift and qudit-flip errors. These two types of errors are not equally likely, and it is desirable to construct quantum codes with a higher correction capability for phase-shift errors [25].

In this work, we provide EAQECCs with excellent parameters coming from different con-

structions. In the Euclidean case, we are able to obtain both symmetric and asymmetric EAQECCs with excellent parameters from subfield subcodes of projective Reed-Solomon codes. A key fact for the construction of these codes and the computation of their parameters is the knowledge of the parameters and structure of both the primary and dual codes. We also obtain QECCs, i.e. EAQECCs without entanglement assistance, from subfield subcodes of projective Reed-Solomon codes in some cases. By considering the Hermitian inner product we are also able to obtain codes with excellent parameters. In fact, we produce new parameters according to [21]. Furthermore, as we are giving several different constructions using subfield subcodes of projective Reed-Solomon codes, this contributes to expanding the known constellation of parameters for EAQECC.

Finally, we consider the codes in [18], Reed-Solomon, and BCH codes obtained by evaluating at the roots of a trace function. We consider the projective version of the codes in [18], that is, the subfield subcodes of projective Reed-Solomon codes evaluating at the roots of a trace function and the point at infinity. This allows us to give classical linear codes which are record in [21], and new EAQECCs.

Our results can be summarized as follows.

- We consider projective Reed-Solomon codes over the zero locus of $x^N - x$ (and the point at infinity), where we evaluate an arbitrary set of monomials. We obtain bases for the subfield subcodes of these codes in Theorem B.3.4.
- When $p \mid N$, bases for the duals of the subfield subcodes are obtained in Theorem B.4.14.
- Considering sets of monomials whose exponents are a union of consecutive cyclotomic sets and the next minimal element, we obtain EAQECCs with entanglement parameter $c \leq 1$ in Theorem B.5.5 and Theorem B.5.15. Some of the resulting codes improve the table for EAQECCs from [21].
- Assuming $p \mid N$, by considering the sets of monomials $\{0, 1, \ldots, d_i\}$, for some $1 \leq d_1, d_2 \leq N - 1$, we obtain asymmetric EAQECCs with entanglement parameter $c = 1$, which compare favorably with the current literature.
- By evaluating in the zeroes of the trace function, plus the point at infinity, and evaluating monomials whose exponents are a union of consecutive cyclotomic sets and the next minimal element, we obtain linear codes with good parameters in Theorem B.6.4, some of which improve the best known parameters in [21], see Example B.6.5. Moreover, we obtain EAQECCs with good parameters and entanglement parameter $c \leq 1$ in Theorem B.6.6.

B.2 Preliminaries

We consider a finite field $\mathbb{F}_q$ of q elements with characteristic p, and its degree s extension $\mathbb{F}_{q^s}$, with $s \geq 1$. We consider the affine space $\mathbb{A}^1$ over $\mathbb{F}_{q^s}$ and the polynomial ring $R = \mathbb{F}_{q^s}[x]$. We choose a set of elements $Y = \{Q_1, \ldots, Q_n\} \subset \mathbb{A}^1$ and its vanishing ideal $I(Y) = \langle \prod_{i=1}^{n}(x - Q_i) \rangle$, where we are regarding the points of $\mathbb{A}^1$ as elements in $\mathbb{F}_{q^s}$. We define the following evaluation map

$$\mathrm{ev}_Y : R/I(Y) \to \mathbb{F}_{q^s}^n, \;\; f \mapsto (f(Q_1), \ldots, f(Q_n))_{Q_i \in Y}\,.$$

where we denote a polynomial and its class in the quotient ring $R/I(Y)$ in the same way. Let Δ be a subset of $\{0, 1, \ldots, n-1\}$. Then, the Reed-Solomon code associated to Δ and

Y, denoted by $\mathrm{RS}(Y, \Delta)$, is the code generated by

$$\{\mathrm{ev}_Y(x^i) \mid i \in \Delta\}.$$

The usual choices are $\Delta = \{0, 1 \ldots, d\}$ and $Y = \mathbb{F}_{q^s}^* = \mathbb{F}_{q^s} \setminus \{0\}$, which give a Reed-Solomon code with parameters $[q^s - 1, d + 1, q^s - d - 1]$. This code can be extended by evaluating at 0 as well, obtaining a code with parameters $[q^s, d + 1, q^s - d]$.

Let $N > 1$ be such that $N - 1 \mid q^s - 1$. We can consider the set of points $Y_N^* = \{Q_1, \ldots, Q_N\}$ given by the zero locus of $I(Y_N^*) = \langle x^{N-1} - 1 \rangle$. In this case, Y_N^* forms a multiplicative subgroup of $\mathbb{F}_{q^s}^*$ and it is already known how to obtain bases for its subfield subcodes (see, for example, [22, 24]). Moreover, BCH codes can be defined as the duals of the subfield subcodes of Reed-Solomon codes when we evaluate in a subgroup Y_N^* [2]. Indeed, let $\alpha \in \mathbb{F}_{q^s}$ be a primitive $(N-1)$th root of unity. C is a BCH code of designed distance δ if it has as generator polynomial the least common multiple of the minimal polynomials of the $\delta - 1$ consecutive elements $\alpha^b, \alpha^{b+1}, \ldots, \alpha^{b+\delta-2}$, with $b \geq 1$, which implies that C is formed by the vectors over $\mathbb{F}_q^{N-1}$ that are orthogonal to the rows of the matrix

$$H = \begin{pmatrix} 1 & \alpha^b & \alpha^{2b} & \cdots & \alpha^{(N-2)b} \\ 1 & \alpha^{b+1} & \alpha^{2(b+1)} & \cdots & \alpha^{(N-2)(b+1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^{b+\delta-2} & \alpha^{2(b+\delta-2)} & \cdots & \alpha^{(N-2)(b+\delta-2)} \end{pmatrix}. \tag{B.2.1}$$

However, this is precisely the generator matrix of the Reed Solomon code over $\mathbb{F}_{q^s}$ with $\Delta = \{b, b + 1, \ldots, b + \delta - 2\}$ and $Y = Y_N^*$. Furthermore, the vectors in $\mathbb{F}_q^{N-1}$ that are orthogonal to the rows of H are precisely the vectors of the subfield subcode of the dual code of this Reed-Solomon code, which is therefore equal to the aforementioned BCH code. In this situation, we say that H is a *pseudo parity check-matrix* for C.

Because of the previous discussion, throughout this work we will focus on evaluating in subgroups of the form Y_N^* unless stated otherwise. As before, we can also include the evaluation of 0, which corresponds to considering instead the set Y_N, the zero locus of $I(Y_N) = \langle x^N - x \rangle$. For the Reed-Solomon codes obtained by evaluating the associated monomials to Δ in Y_N we will use the notation $\mathrm{RS}(N, \Delta)$. The subfield subcode of the code $\mathrm{RS}(N, \Delta)$ over $\mathbb{F}_q$ is denoted by $\mathrm{RS}(N, \Delta)_q := \mathrm{RS}(N, \Delta) \cap \mathbb{F}_q^N$. In this case, for the sake of simplicity, we are also going to denote $R_N := R/I(Y_N)$.

Now we are going to introduce some necessary definitions in order to obtain bases for the codes $\mathrm{RS}(N, \Delta)_q$. We define $\mathbb{Z}_N = \{0\} \cup \mathbb{Z}/\langle N - 1 \rangle$, where we represent the classes of $\mathbb{Z}/\langle N - 1 \rangle$ by $\{1, \ldots, N\}$. A subset $\mathfrak{I}$ of $\mathbb{Z}_N$ is called a *cyclotomic set* with respect to q if $q \cdot z \in \mathfrak{I}$ for any $z \in \mathfrak{I}$. $\mathfrak{I}$ is said to be minimal (with respect to q) if it can be expressed as $\mathfrak{I} = \{q^i \cdot z, i = 1, 2, \ldots\}$ for a fixed $z \in \mathfrak{I}$, and in that situation we will write $\mathfrak{I}_z := \mathfrak{I}$ and $n_z = |\mathfrak{I}_z|$. We say z is a *minimal representative* of $\mathfrak{I}_z$ if z is the least element in $\mathfrak{I}_z$, and we will say it is a *maximal representative* of $\mathfrak{I}_z$ if it is the biggest element. We will denote by $\mathcal{A}$ the set of minimal representatives of the minimal cyclotomic cosets, and by $\mathcal{B}$ the set of maximal representatives of the minimal cyclotomic cosets.

Example B.2.1. Consider the extension $\mathbb{F}_9 \supset \mathbb{F}_3$. We consider $N = 9$ and we have $\mathbb{Z}_N = \{0\} \cup \mathbb{Z}/\langle 8 \rangle$. We have the following minimal cyclotomic sets:

$$\mathfrak{I}_0 = \{0\}, \mathfrak{I}_1 = \{1, 3\}, \mathfrak{I}_2 = \{2, 6\}, \mathfrak{I}_4 = \{4\}, \mathfrak{I}_5 = \{5, 7\}, \mathfrak{I}_8 = \{8\}.$$

The set of minimal representatives is $\mathcal{A} = \{0, 1, 2, 4, 5, 8\}$, and the set of maximal representatives is $\mathcal{B} = \{0, 3, 4, 6, 7, 8\}$.

The dimension of the subfield subcodes of Reed-Solomon codes is already present in [22]. For the codes $\mathrm{RS}(N, \Delta)_q$ it is possible to obtain a basis given by the evaluation of some polynomials. For each $a \in \mathcal{A}$, we define the following trace map:

$$\mathcal{T}_a : R_N \to R_N, \;\; f \mapsto f + f^q + \cdots + f^{q^{(n_a-1)}},$$

and given $\Delta \subset \{0, 1, \ldots, N-1\}$, we denote $\Delta_{\mathfrak{J}} := \bigcup_{\mathfrak{J}_a \subset \Delta} \mathfrak{J}_a \subset \Delta$. The following result gives a basis for the code $\mathrm{RS}(N, \Delta)_q$ [13, Thm. 11].

Theorem B.2.2. *Let Δ be a subset of $\{0, 1, \ldots, N-1\}$ and set ξ_a a primitive element of the field $\mathbb{F}_{q^{n_a}}$. Then, a basis of the vector space $\mathrm{RS}(N, \Delta)_q$ is given by the images under the map ev_{Y_N} of the set of classes in R_N*

$$\bigcup_{a \in \mathcal{A} | \mathfrak{J}_a \subset \Delta} \{\mathcal{T}_a(\xi_a^r x^a) \mid 0 \leq r \leq n_a - 1\}.$$

As a consequence, we have that

$$\dim \mathrm{RS}(N, \Delta)_q = \sum_{\mathfrak{J}_z : \mathfrak{J}_z \subset \Delta} n_z = |\Delta_{\mathfrak{J}}|.$$

Having seen the affine setting, we are now going to introduce the codes we are going to use throughout this work. We consider the projective line $\mathbb{P}^1$ over $\mathbb{F}_{q^s}$ and the polynomial ring $S = \mathbb{F}_{q^s}[x_0, x_1]$. Given a degree $d \geq 1$, we denote by S_d the homogeneous polynomials of degree d. We are going to fix representatives for the points of $\mathbb{P}^1$ in the following way: for each point $[P] \in \mathbb{P}^1$, we choose the representative whose first nonzero coordinate is equal to 1. We will denote by P^1 this set of representatives, seen as points in the affine space $\mathbb{A}^2$, and we will call them *standard representatives*. If we also consider a finite set of points $X = \{Q_1, \ldots, Q_n\} \subset P^1$, we can define the following evaluation map

$$\mathrm{ev}_X : S/I(X) \to \mathbb{F}_{q^s}^n, \;\; f \mapsto (f(Q_1), \ldots, f(Q_n))_{Q_i \in X},$$

where, as before, we denote a polynomial in S and its class in $S/I(X)$ in the same way. Given $\Delta \subset \{0, 1, \ldots, n-1\}$, we define $d(\Delta) := \max\{i \mid i \in \Delta\}$. The *projective Reed-Solomon* code associated to Δ and X is the code generated by

$$\{\mathrm{ev}_X(x_0^{d(\Delta)-i} x_1^i) \mid i \in \Delta\},$$

which will be denoted by $\mathrm{PRS}(X, \Delta)$. We note that we are only evaluating monomials of exactly degree $d(\Delta)$, which means that their linear combinations are homogeneous polynomials of degree $d(\Delta)$. If $0 \notin \Delta$, $\mathrm{PRS}(X, \Delta)$ is a degenerate code because all the previous monomials would evaluate to 0 at the point $[1 : 0]$. Therefore, we are always going to assume in what follows that $0 \in \Delta$. Some authors define these codes over the projective space without fixing representatives, as in [30], but then they can only define the code up to monomial equivalence. Monomially equivalent codes do not necessarily have monomially equivalent subfield subcodes, for example in [23] the authors see that

the dimension of the subfield subcode of a generalised Reed-Solomon code depends on the twist vector chosen, and that is why we fix representatives from the beginning.

Given a degree $1 \leq d \leq q^s$, the most standard definition of projective Reed-Solomon code in the literature is the code $\mathrm{PRS}(P^1, \Delta_d)$, where $\Delta_d := \{0, 1, \ldots, d\}$. The code $\mathrm{PRS}(P^1, \Delta_d)$ is also called *doubly extended Reed-Solomon code* and its parameters are $[q^s + 1, d + 1, q^s - d + 1]$.

In order to obtain bases for the subfield subcodes of the codes $\mathrm{PRS}(X, \Delta)$, we are going to evaluate in subgroups similarly to the affine case. The natural ideal is to add the point at infinity $[0 : 1]$ to the points that we were considering in the affine case. Therefore, given N such that $N - 1 \mid q^s - 1$, we define $\mathbb{X}_N^* = [\{1\} \times Y_N^*] \cup [0 : 1] \subset \mathbb{P}^1$ and $\mathbb{X}_N = [\{1\} \times Y_N] \cup [0 : 1] \subset \mathbb{P}^1$, where we recall that Y_N^* and Y_N are the zero locus of $\langle x^{N-1} - 1 \rangle$ and $\langle x^N - x \rangle$, respectively. However, it is easy to see that another set of representatives for $\mathbb{X}_N^*$ is $[Y_N \times \{1\}]$. Thus, the codes obtained when evaluating in this set would be monomially equivalent to the ones obtained in the affine case when evaluating in Y_N. As we said before, this does not mean that their subfield subcodes are monomially equivalent. Nevertheless, our experiments show that the parameters that we obtain when evaluating in the set $\mathbb{X}_N^*$ are strictly worse than the ones obtained in the affine case with Y_N. Hence, in what follows we are going to focus on evaluating in the set $\mathbb{X}_N$, although we note that the theory we are going to develop can be adapted for the set $\mathbb{X}_N^*$ as well.

We denote the standard representatives of $\mathbb{X}_N$ by X_N, and we also denote $\mathrm{PRS}(N, \Delta) := \mathrm{PRS}(X_N, \Delta)$. With this notation, doubly extended Reed-Solomon codes are denoted by $\mathrm{PRS}(q^s, \Delta_d)$. Similarly to the case of doubly extended Reed-Solomon codes, given $1 \leq d \leq N$, the parameters of the code $\mathrm{PRS}(N, \Delta_d)$ are $[N + 1, d + 1, N - d + 1]$. In general, for the codes $\mathrm{PRS}(N, \Delta)$ we have the parameters $[N + 1, |\Delta|, \geq N - d(\Delta) + 1]$, where the bound for the minimum distance is given by the smallest doubly extended Reed-Solomon code that contains $\mathrm{PRS}(N, \Delta)$.

B.3 Subfield subcodes of codes over the projective line

Let $\mathbb{F}_{q^s} \supset \mathbb{F}_q$ and N such that $N - 1 \mid q^s - 1$. In this section we want to obtain bases for the subfield subcodes of the codes $\mathrm{PRS}(N, \Delta)$ with respect to this extension, which we will denote by $\mathrm{PRS}(N, \Delta)_q := \mathrm{PRS}(N, \Delta) \cap \mathbb{F}_q$. Given $f \in S$, we say that f evaluates to $\mathbb{F}_q$ in X_N whenever $f(Q) \in \mathbb{F}_q$ for all $Q \in X_N$ (similarly for polynomials in R evaluating in Y_N). The following lemma gives the key idea in order to obtain bases for $\mathrm{PRS}(N, \Delta)_q$.

Lemma B.3.1. *Let $X_N \subset P^1$. Then $f \in S$ evaluates to $\mathbb{F}_q$ in $X_N \iff f(1, x_1)$ evaluates to $\mathbb{F}_q$ in Y_N and $f(0, 1)$ is in $\mathbb{F}_q$.*

We will see now that we can take advantage of the knowledge from the affine case in Theorem B.2.2 by homogenizing and using Lemma B.3.1. Given a degree d and a polynomial $f(x) \in R$ with $\deg(f) \leq d$, its homogenization up to degree d is the homogeneous polynomial $f^h(x_0, x_1) := x_0^d f(x_1/x_0) \in S_d$. Unless stated otherwise, when we consider the code $\mathrm{PRS}(N, \Delta)$, we are always going to assume that we are homogenizing up to degree $d = d(\Delta)$.

For a polynomial $f \in \mathbb{F}_q[x_1]$, we choose $\mathcal{T}_a(f)$ as the representative of the class in $\mathbb{F}_{q^s}[x_1]/I(Y_N)$ which has the exponents of each monomial reduced modulo $q^s - 1$. Given $d \geq 1$, if the degree of $\mathcal{T}_a(f)$ is lower than d, then we define $\mathcal{T}_a^h(f) := (\mathcal{T}_a(f))^h$, which we

call homogenized trace. If we consider one of the traces that appear in Theorem B.2.2, its homogenized trace automatically satisfies that, when setting $x_0 = 1$, the resulting polynomial evaluates to $\mathbb{F}_q$ in Y_N, i.e., the first condition from Lemma B.3.1 is satisfied. However, the second condition, which means that the coefficient of x_1^d in the homogenized trace must be in $\mathbb{F}_q$, might not be satisfied. Because of this, the projective case is more involved than the affine case, as we will see in the next example.

Example B.3.2. We continue with Example B.2.1. By Theorem B.2.2, the following polynomial associated to $\mathfrak{I}_1$ evaluates to $\mathbb{F}_3$:

$$\mathcal{T}_1(x) = x + x^3.$$

Let $d = 3$ (the degree up to which we homogenize). If we consider the polynomial $f = \mathcal{T}_1^h(x_1) = x_0^2 x_1 + x_1^3$, this is a homogeneous polynomial of degree 3 such that $f(1, x_1)$ takes the same values as $\mathcal{T}_1(x_1)$ in $\mathbb{F}_9$, and $f(0, 1) = 1 \in \mathbb{F}_3$. By Lemma B.3.1, we know that f evaluates to $\mathbb{F}_3$ when evaluating in P^1.

If ξ is a primitive element in $\mathbb{F}_9$, by Theorem B.2.2, the following polynomial also evaluates to $\mathbb{F}_3$:

$$\mathcal{T}_1(\xi x) = \xi x + \xi^3 x^3.$$

However, if we consider $g = \mathcal{T}_1^h(\xi x_1) = \xi x_0^2 x_1 + \xi^3 x_1^3$, we see that $g(0, 1) = \xi^3 \notin \mathbb{F}_3$. Therefore g does not evaluate to $\mathbb{F}_3$.

Remark B.3.3. If we have $f \in S_d$ which evaluates to $\mathbb{F}_q$, then $x_0 f \in S_{d+1}$ also evaluates to $\mathbb{F}_q$. Moreover, if $f(1, x_1)$ evaluates to $\mathbb{F}_q$ in Y_N, then $g = x_0 f \in S_{d+1}$ evaluates to $\mathbb{F}_q$ in X_N, even if f does not, because $g(1, x_1) = f(1, x_1)$, which evaluates to $\mathbb{F}_q$, and $g(0, 1) = 0 \in \mathbb{F}_q$. This already gives a hint about the fact that the sequence of dimensions of the subfield subcodes is going to be non-decreasing.

With Lemma B.3.1, we can consider polynomials in one variable that evaluate to $\mathbb{F}_q$ in order to obtain polynomials in S_d that evaluate to $\mathbb{F}_q$ in X_N in some cases. One could also consider the polynomials in two variables that evaluate to $\mathbb{F}_q$ when evaluating in the points of $\mathbb{A}^2$. All of those polynomials are going to evaluate to $\mathbb{F}_q$ when evaluating in points of P^1. However, there are bivariate polynomials that evaluate to $\mathbb{F}_q$ in P^1, but not in $\mathbb{A}^2$. For example, in Example B.3.2 we consider $f = x_0^2 x_1 + x_1^3$, which evaluates to $\mathbb{F}_3$ over P^1, but if we consider this polynomial over $\mathbb{A}^2$, then it is clear that it does not evaluate to $\mathbb{F}_3$. For example, if ξ is a primitive element in $\mathbb{F}_9$, $f(0, \xi) = \xi^3 \notin \mathbb{F}_3$.

The following result shows how to use the previous ideas to obtain a basis for $\mathrm{PRS}(N, \Delta)_q$.

Theorem B.3.4. *Let Δ be a nonempty subset of $\{0, 1, \ldots, N-1\}$ and let $d = d(\Delta)$. Set ξ_b a primitive element of the field $\mathbb{F}_{q^{n_b}}$. A basis for $\mathrm{PRS}(N, \Delta)_q$ is given by the image by ev_{X_N} of the following polynomials.*

If $\mathfrak{I}_d \subset \Delta$:

$$\bigcup_{b \in \mathcal{B} | \mathfrak{I}_b \subset \Delta, b < d} \{\mathcal{T}_b^h(\xi_b^r x_1^b) \mid 0 \leq r \leq n_b - 1\} \cup \{\mathcal{T}_d^h(x_1^d)\}.$$

If $\mathfrak{I}_d \not\subset \Delta$:

$$\bigcup_{b \in \mathcal{B} | \mathfrak{I}_b \subset \Delta} \{\mathcal{T}_b^h(\xi_b^r x_1^b) \mid 0 \leq r \leq n_b - 1\}.$$

Proof. If we consider

$$\bigcup_{b\in\mathcal{B}|\mathfrak{I}_b\subset\Delta, b<d} \{\mathcal{T}_b^h(\xi_b^r x_1^b) \mid 0 \leq r \leq n_b - 1\},$$

these are functions which have linearly independent evaluations, because when evaluating in $[\{1\} \times X_N]$ they are linearly independent by Theorem B.2.2. These polynomials do not have the monomial x_1^d in their support. Therefore, by Lemma B.3.1, they evaluate to $\mathbb{F}_q$ in X_N.

If $\mathfrak{I}_d \not\subset \Delta$, we are going to see that the evaluation of these polynomials generates the whole subfield subcode. Let $S_{d,\Delta} \subset S_d$ be the linear space generated by $\{x_0^{d-i}x_1^i \mid i \in \Delta\}$, and let $f \in S_{d,\Delta}$ be such that its evaluation is in $\mathrm{PRS}(N,\Delta)_q$. If $f(0,1) = 0$, then, using Theorem B.2.2, we know that we can generate the evaluation of f with these polynomials. On the other hand, we claim that $f(0,1) \neq 0$ cannot happen in this case, which means that the image by the evaluation map of the stated polynomials generate the whole subfield subcode. If we had $f(0,1) \neq 0$, that would imply that $f(1,x_1)$ has the monomial x_1^d in its support. However, if $\mathfrak{I}_d \not\subset \Delta$, then we know that there is at least one $a_1 \in \mathfrak{I}_d$ which is not in Δ. Therefore, we cannot obtain the monomial $x_1^{a_1}$ in the support of $f(1,x_1)$ because using Theorem B.2.2 in Y_N, once you have x_1^d in the support of $f(1,x_1)$, you should have x_1^a in its support for all $a \in \mathfrak{I}_d$ because $f(1,x_1)$ should be a linear combination of traces. Therefore, $f(0,1) \neq 0$ is not possible in this case, and the stated polynomials generate the whole subfield subcode.

In the case $\mathfrak{I}_d \subset \Delta$ we have that $d \in \mathcal{B}$, i.e., there is a minimal cyclotomic set whose maximal representative is equal to d. By Lemma B.3.1, we have that $\mathcal{T}_d^h(x_1^d)$ evaluates to $\mathbb{F}_q$, and it is linearly independent from the other polynomials that we consider because it is the only one that takes a nonzero value at $[0:1]$.

We are going to show now that the evaluation of the given set of polynomials generates the whole code in this case. Let $f \in S_{d,\Delta}$ such that f evaluates to $\mathbb{F}_q$. By Lemma B.3.1, $f(0,1)$ is in $\mathbb{F}_q$. Hence, we can subtract $\mathcal{T}_d^h(x_1^d)$ multiplied by $f(0,1) \in \mathbb{F}_q$ and the evaluation would still be in $\mathbb{F}_q$. Therefore, we can assume that f does not have the monomial x_1^d in its support, i.e., $f(0,1) = 0$. Then we can use the affine case and argue that if $f(1,x_1)$ evaluates to $\mathbb{F}_q$, by Theorem B.2.2 it must be a linear combination of the polynomials in

$$\bigcup_{b\in\mathcal{B}|\mathfrak{I}_b\subset\Delta, b<d} \{\mathcal{T}_b(\xi_b^r x_1^b) \mid 0 \leq r \leq n_b - 1\}.$$

The homogenized polynomials that we consider have the same evaluation as these polynomials in $[\{1\} \times Y_N]$, which completes the proof. □

Remark B.3.5. We note that we are obtaining a basis which is the image by the evaluation map of some homogeneous polynomials of degree d, which we already knew that should be possible because $\mathrm{PRS}(N,\Delta)_q \subset \mathrm{PRS}(N,\Delta)$.

Example B.3.6. We continue with Examples B.2.1 and B.3.2. We consider $N = 9$ and $\Delta = \{0,1,2,3\}$, which means that we have $d(\Delta) = 3$. Looking at the cyclotomic sets from Example B.2.1, we see that $\mathfrak{I}_0 \cup \mathfrak{I}_1 \subset \Delta$ (and these are the only complete minimal cyclotomic sets in Δ). By Theorem B.3.4, taking into account that in this case we have

$\mathfrak{I}_3 = \mathfrak{I}_d \subset \Delta$, we see that the evaluation of the following polynomials is a basis for $\mathrm{PRS}(9, \Delta)_3$:

$$\mathcal{T}_0^h(x_1^0) = x_0^3, \mathcal{T}_3^h(x_1^3) = x_0^2 x_1 + x_1^3.$$

We note that the second polynomial is precisely the polynomial f in Example B.3.2.

If we take $\Delta = \{0, 1, 2, 3, 4\}$, then we have $d(\Delta) = 4$ and $\mathfrak{I}_0 \cup \mathfrak{I}_1 \cup \mathfrak{I}_4 \subset \Delta$. By Theorem B.3.4, the evaluation of the following polynomials is a basis for $\mathrm{PRS}(9, \Delta)_3$:

$$\mathcal{T}_0^h(x_1^0) = x_0^4, \mathcal{T}_3^h(x_1^3) = x_0^3 x_1 + x_0 x_1^3, \mathcal{T}_3^h(\xi x_1^3) = \xi^3 x_0^3 x_1 + \xi x_0 x_1^3, \mathcal{T}_4^h(x_1^4) = x_1^4.$$

Corollary B.3.7. *The dimension of* $\mathrm{PRS}(N, \Delta)_q$ *is the following:*

$$\dim \mathrm{PRS}(N, \Delta)_q = \begin{cases} \displaystyle\sum_{b \in \mathcal{B}: \mathfrak{I}_b \subset \Delta} n_b - (n_d - 1) = \sum_{b \in \mathcal{B}: \mathfrak{I}_b \subset \Delta, b < d} n_b + 1 & \text{if } \mathfrak{I}_d \subset \Delta \\ \displaystyle\sum_{b \in \mathcal{B}: \mathfrak{I}_b \subset \Delta} n_b & \text{otherwise} \end{cases}$$

Remark B.3.8. Let $d = d(\Delta)$. If $\mathfrak{I}_d \subset \Delta$, we have dimension 1 more than in the affine case with $\Delta \setminus \{d\}$. On the other hand, if $\mathfrak{I}_d \not\subset \Delta$, we obtain a degenerate code with a 0 at the point $[0 : 1]$. Therefore, the interesting case is when $\mathfrak{I}_d \subset \Delta$, which is the one in which we are going to mainly focus in what follows.

With respect to the minimum distance, if we denote by $\mathrm{wt}(C)$ the minimum distance of a code $C \subset \mathbb{F}_{q^s}^n$, we have $\mathrm{wt}(\mathrm{PRS}(N, \Delta)) \geq N - d(\Delta) + 1$, which implies that $\mathrm{wt}(\mathrm{PRS}(N, \Delta)_q) \geq N - d(\Delta) + 1$ because $\mathrm{PRS}(N, \Delta)_q \subset \mathrm{PRS}(N, \Delta)$. For the case of subfield subcodes of doubly extended Reed-Solomon codes we obtain the following corollary.

Corollary B.3.9. *Let* $d \in \mathcal{B}$. *The parameters of* $\mathrm{PRS}(q^s, \Delta_d)_q$ *are* $[q^s + 1, \displaystyle\sum_{b \in \mathcal{B}: b < d} n_b + 1, \geq q^s - d + 1]$. *Moreover, the first nontrivial (dimension higher than 1) subfield subcode is obtained when* $d = q^{s-1}$.

Proof. The parameters are a special case of the previous results and discussions. For the last statement, it is clear that $q^s/q = q^{s-1}$ is the lowest possible element in $\mathcal{B}$ (besides 0), and $d = q^{s-1}$ is the first degree such that $\mathfrak{I}_1 = \{1, q, q^2, \ldots, q^{s-1}\} \subset \Delta_d$. □

The bound used for the minimum distance of the subfield subcodes of doubly extended Reed-Solomon codes is sharp in all cases we have checked with $d \in \mathcal{B}$. The codes obtained in this way have one more length and dimension than in the affine case, with the same minimum distance.

Example B.3.10. If we look at the results from Example B.3.6, we see that we obtained dimension 2 and 4 for $\mathrm{PRS}(9, \Delta_3)_3$ and $\mathrm{PRS}(9, \Delta_4)_3$. These are the values obtained with Corollary B.3.9, because $2 = n_0 + 1$ and $4 = n_0 + n_3 + 1$. We would obtain codes with parameters $[10, 2, 7]$ and $[10, 4, 6]$ over $\mathbb{F}_3$.

B.4 Dual codes of the previous subfield subcodes

In order to compute the dual codes of the previous subfield subcodes, we are going to use Delsarte's Theorem [10].

Theorem B.4.1. *Let $C \subset \mathbb{F}_{q^s}^n$ be a linear code.*

$$(C \cap \mathbb{F}_q^n)^\perp = \mathrm{Tr}(C^\perp),$$

where $\mathrm{Tr} : \mathbb{F}_{q^s} \to \mathbb{F}_q$*, which maps x to $x + x^q + \cdots + x^{q^{s-1}}$, is applied componentwise to $C^\perp$.*

In order to use this result, we need to compute the dual of the codes $\mathrm{PRS}(N, \Delta)$. It is well known that $\mathrm{PRS}(q^s, \Delta_d)^\perp = \mathrm{PRS}(q^s, \Delta_{q^s-1-d})$ (the dual of a doubly extended Reed-Solomon code is another doubly extended Reed-Solomon code). However, computing the dual of the codes $\mathrm{PRS}(N, \Delta)$ in general can be involved. Nevertheless, we can easily compute the dual in some cases. In order to do so, we are going to state the metric structure of these codes first. Part of the following result already appears in [17, Prop. 1] and [28, Lem. 7.1].

Lemma B.4.2. *Let γ be a non-negative integer, and N such that $N - 1 \mid q^s - 1$. We consider the monomial $x^\gamma \in \mathbb{F}_{q^s}[x]$. We have the following:*

$$\sum_{z \in Y_N} x^\gamma(z) = \begin{cases} N & \text{if } \gamma = 0, \\ 0 & \text{if } \gamma > 0 \text{ and } \gamma \not\equiv 0 \bmod (N-1), \\ N-1 & \text{if } \gamma > 0 \text{ and } \gamma \equiv 0 \bmod (N-1). \end{cases}$$

Proof. Let $\xi \in \mathbb{F}_{q^s}$ be an element of order $N - 1$, which exists because $N - 1 \mid q^s - 1$. Then $Y_N = \{\xi^0, \xi^1, \ldots, \xi^{N-2}\} \cup \{0\}$. If $\gamma = 0$, $x^\gamma = 1$, and the sum is equal to $|Y_N| = N$. If $\gamma > 0$ and $\gamma \equiv 0 \bmod (N-1)$, then $x^\gamma(z) = 1$ for all $z \in Y_N \setminus \{0\}$, and $\sum_{z \in Y_N} x^\gamma(z) = |Y_N| - 1 = N - 1$. Finally, if $\gamma > 0$ and $\gamma \not\equiv 0 \bmod (N-1)$, we have

$$\sum_{z \in Y_N} x^\gamma(z) = \sum_{i=0}^{N-2} (\xi^i)^\gamma = \frac{\xi^{\gamma(N-1)} - 1}{\xi^\gamma - 1} = 0.$$

□

Proposition B.4.3. *Let $x_0^{\alpha_0} x_1^{\alpha_1}$ and $x_0^{\beta_0} x_1^{\beta_1}$ be two monomials in $\mathbb{F}_{q^s}[x_0, x_1]$ of degree d_α and d_β, respectively. Then we have the following for the product of the evaluations over X_N. If $\alpha_1 + \beta_1 = 0$:*

$$\mathrm{ev}_{X_N}(x_0^{\alpha_0} x_1^{\alpha_1}) \cdot \mathrm{ev}_{X_N}(x_0^{\beta_0} x_1^{\beta_1}) = \begin{cases} N+1 & \text{if } \alpha_0 + \beta_0 = 0, \\ N & \text{if } \alpha_0 + \beta_0 > 0. \end{cases}$$

If $\alpha_1 + \beta_1 > 0$:

$$\mathrm{ev}_{X_N}(x_0^{\alpha_0} x_1^{\alpha_1}) \cdot \mathrm{ev}_{X_N}(x_0^{\beta_0} x_1^{\beta_1}) = \begin{cases} N & \text{if } \alpha_1 + \beta_1 \equiv 0 \bmod (N-1), \alpha_0 + \beta_0 = 0, \\ N-1 & \text{if } \alpha_1 + \beta_1 \equiv 0 \bmod (N-1), \alpha_0 + \beta_0 > 0, \\ 1 & \text{if } \alpha_1 + \beta_1 \not\equiv 0 \bmod (N-1), \alpha_0 + \beta_0 = 0, \\ 0 & \text{if } \alpha_1 + \beta_1 \not\equiv 0 \bmod (N-1), \alpha_0 + \beta_0 > 0. \end{cases}$$

Proof. First, we expand the scalar product as a sum over $X_N = \{[1 : z] \mid z \in Y_N\} \cup \{[0 : 1]\} \subset P^1$:

$$\mathrm{ev}_{X_N}(x_0^{\alpha_0} x_1^{\alpha_1}) \cdot \mathrm{ev}_{X_N}(x_0^{\beta_0} x_1^{\beta_1}) = \sum_{P \in X_N} x_0^{\alpha_0+\beta_0} x_1^{\alpha_1+\beta_1}(P) = \sum_{z \in Y_N} z^{\alpha_1+\beta_1} + \epsilon,$$

where ϵ is equal to 1 if $\alpha_0 + \beta_0 = 0$ and equal to 0 if $\alpha_0 + \beta_0 > 0$ (corresponding to the evaluation at $[0 : 1]$). The result is obtained by using Lemma B.4.2. □

If p does not divide N, we have that the evaluation of $x_1^{\alpha_1}$ with $\alpha_1 > 0$ is not orthogonal to the evaluation of $x_1^{\beta_1}$ for any β_1. This means that the dual code $\mathrm{PRS}(N, \Delta)^\perp$ does not have a basis obtained by the evaluation of monomials unless $\mathrm{wt}(\mathrm{PRS}(N, \Delta)) = 1$. This is because if we have $\mathrm{wt}(\mathrm{PRS}(N, \Delta)) > 1$, then $\mathrm{PRS}(N, \Delta)^\perp$ cannot be degenerate. In particular, there must be a vector in $\mathrm{PRS}(N, \Delta)^\perp$ such that the coordinate associated to the point $[0 : 1]$ is nonzero, which is obtained by evaluating a polynomial with some power of x_1 in its support, but it cannot be just a single power of x_1 because its evaluation would not be orthogonal to the evaluation of x_1^d. Hence, the dual code is not generated by the image by the evaluation map of monomials.

When $p \mid N$, as the next result shows, the previous result gets simplified, and in Proposition B.4.10 we will see that in this case the dual code can be generated by the evaluation of monomials.

Corollary B.4.4. *If $p \mid N$, then:*

$$\mathrm{ev}_{X_N}(x_0^{\alpha_0} x_1^{\alpha_1}) \cdot \mathrm{ev}_{X_N}(x_0^{\beta_0} x_1^{\beta_1}) = \begin{cases} 1 & \text{if } \alpha_1 + \beta_1 = 0, \alpha_0 + \beta_0 = 0 \text{ or} \\ & \quad \alpha_1 + \beta_1 \not\equiv 0 \mod (N-1), \alpha_0 + \beta_0 = 0, \\ -1 & \text{if } \alpha_1 + \beta_1 \equiv 0 \mod (N-1), \alpha_i + \beta_i > 0, i = 0, 1, \\ 0 & \text{otherwise.} \end{cases}$$

Remark B.4.5. One way to have $p \mid N$ is to consider a subfield of $\mathbb{F}_{q^s}$, in which case we are going to obtain a doubly extended Reed-Solomon code over that subfield. However, we may also have $p \mid N$ for different subgroups of $\mathbb{F}_{q^s}^*$. For example, if we consider $q^s = 2^4 = 16$, then 5 divides $q^s - 1$. Therefore, we can take $N = 6$, which is divisible by 2, but Y_6 is not a subfield of $\mathbb{F}_{16}$.

For obtaining a basis for the dual code we will need to work with non-homogeneous polynomials. In order to understand linear independence in that situation we are going to introduce now a universal Gröbner basis for the vanishing ideal $I(X_N)$. Particular cases of the following result were already present in [31].

Proposition B.4.6. *A universal Gröbner basis for the ideal $I(X_N)$ is:*

$$I(X_N) = \langle x_0^2 - x_0, x_1^N - x_1, (x_0 - 1)(x_1 - 1) \rangle.$$

Therefore, $\mathrm{in}(I(X_N)) = \langle x_0^2, x_1^N, x_0 x_1 \rangle$ *and* $\{1, x_0, x_1, x_1^2, \ldots, x_1^{N-1}\}$ *is a basis for the quotient ring $S/I(X_N)$.*

Proof. First, we are going to show that these polynomials generate the vanishing ideal $I(X_N)$. Given any point in X_N, it is clear that it satisfies the equations. Reciprocally, any point satisfying this equations, because of the generator $x_0^2 - x_0$, must have the first coordinate equal to 0 or 1. If the first coordinate is equal to 0, because of the generator $(x_0 - 1)(x_1 - 1)$, the last coordinate must be 1, i.e., it must be the point $[0 : 1] \in X_N$. If the first coordinate is equal to 1, then, because of the generator $x_1^N - x_1$, the second coordinate is in Y_N, which means that the point is in X_N as well.

We have proved that the variety defined by this ideal is X_N. It is clear that the variety defined by this ideal over the algebraic closure $\overline{\mathbb{F}_{q^s}}$ is the same as the variety defined over $\mathbb{F}_{q^s}$. By Seidenberg's Lemma [26, Prop. 3.7.15], this ideal is radical. Therefore, by Hilbert's Nullstellensatz applied in the algebraic closure, we have that this ideal is the vanishing ideal of the variety that it defines, i.e., is the vanishing ideal of X_N.

In order to show that all the S-polynomials of the generators reduce to 0, we just need to use that if the greatest common divisor of the initial monomials of two polynomials is 1, then their S-polynomial reduces to 0 by [9, Prop. 4, Chapter 2, Section 9]. In particular, if two polynomials depend on different variables, their S-polynomial reduces to 0. And if f and g share a common factor w, then $S(f, g) = wS(f/w, g/w)$. Using this, it is easy to see that all the S-polynomials reduce to 0 in this case, for any monomial order. Thus, these generators form a universal Gröbner basis. The initial ideal follows from this fact, and by Macaulay's classical result [12, Thm. 15.3] we obtain that the monomials not contained in the initial ideal form a basis for the quotient ring. □

Remark B.4.7. Because of the first generator of the previous ideal, any power of x_0 is equivalent to x_0 in the quotient ring. Therefore, we have $x_0^{\alpha_0} x_1^{\alpha_1} \equiv x_0 x_1^{\alpha_1} \bmod I(X_N)$ if $\alpha_0 > 0$. This is why we are going to assume $\alpha_0 = 1$ for any monomial divisible by x_0 in what follows, except when we want to remark that we can obtain a code by evaluating homogeneous polynomials of a certain degree.

The following result allows us to express any polynomial in $S/I(X_N)$ in terms of the basis in Proposition B.4.6.

Lemma B.4.8. *Let a_0, a_1 be integers, with $a_0 > 0$. We have that*

$$x_0^{a_0} x_1^{a_1} \equiv x_0 + x_1^{a_1} - 1 \mod I(X_N).$$

Proof. It is easy to check that both polynomials have the same evaluation in X_N, which implies that they are in the same class modulo $I(X_N)$. □

Corollary B.4.9. *The following monomials constitute a basis for the quotient $S/I(X_N)$:*

$$\{x_1^N, x_0, x_0 x_1, \ldots, x_0 x_1^{N-1}\}.$$

Moreover, every set of the form $\{x_1^d, x_0, x_0 x_1, \ldots, x_0 x_1^{d-1}\}$ with $1 \leq d \leq N$ is linearly independent.

Proof. It is easy to check that these monomials are linearly independent by Lemma B.4.8 and Proposition B.4.6. The fact that for $d = N$ this set is a basis follows from the cardinality of the set and the dimension of the quotient ring. □

Now we have the tools necessary to deal with the dual as an evaluation code over the projective line. In what follows we are going to assume that $p \mid N$. This is because, by Corollary B.4.4, the metric structure is going to be similar to the one of doubly extended Reed-Solomon codes, and in this case the dual code will be generated by the evaluation of monomials. For the following result it will be useful to introduce the definition $\Delta^\perp = \{\alpha \in \{0, 1, \ldots, N-1\} \mid \alpha \neq N - 1 - h, h \in \Delta\}$.

Proposition B.4.10. *Let N be a non-negative integer such that $N - 1 \mid q^s - 1$ and $p \mid N$. Let $\Delta \subset \{0, 1, \ldots, N-1\}$ and let $d = d(\Delta)$. Then $\mathrm{PRS}(N, \Delta)^\perp$ has a basis obtained by taking the image by ev_{X_N} of the following monomials:*

$$\{x_0 x_1^\alpha \mid \alpha \in \Delta^\perp\} \cup \{x_1^{N-1-d}\}. \tag{B.4.1}$$

Moreover, if $N - 1 \notin \Delta$, we can also obtain the same basis by taking the image by ev_{X_N} of the following monomials of degree $2(N-1) - d$ (which allows us to get the dual code as an evaluation code of homogeneous polynomials):

$$\{x_0^{2(N-1)-d-\alpha} x_1^\alpha \mid \alpha \in \Delta^\perp\} \cup \{x_1^{2(N-1)-d}\}. \tag{B.4.2}$$

If $N - 1 \in \Delta$, then the following set of homogeneous polynomials of degree $2N - 1$ give the same image as the set in item (B.4.1)*:*

$$\{x_0^{2N-1-\alpha} x_1^\alpha \mid \alpha \in \Delta^\perp\} \cup \{x_1^{2N-1} + x_0^{2N-1} - x_0^{N-1} x_1^N\}. \tag{B.4.3}$$

Proof. Using Corollary B.4.4 it is easy to see that the evaluation of the monomials in (B.4.1) is orthogonal to the vectors in $\mathrm{PRS}(N, \Delta)$. When $N - 1 \notin \Delta$, using Lemma B.4.8 it is easy to see that the evaluation of these monomials is linearly independent, and the dimension of this subspace is the same as the dimension of the dual code. If $N - 1 \in \Delta$, then $x_1^{N-1-d} = 1$, and it is easy to see that the monomials that we obtain are linearly independent and generate the dual code. When $N - 1 \notin \Delta$, the evaluation of the set (B.4.2) is clearly the same. Finally, if $N - 1 \in \Delta$, we have that

$$x_1^{2N-1} + x_0^{2N-1} - x_0^{N-1} x_1^N \equiv x_1 + x_0 - x_0 x_1 \equiv 1 \mod I(P^1).$$

Therefore, the evaluation of the set (B.4.3) is the same as the one obtained with (B.4.1). □

We have the next result for the case when $p \mid N$, which generalizes what we know about the duality in the case of doubly extended Reed-Solomon codes. We note that, as we are evaluating all the monomials of degree d in the next result, and the set of evaluation points is a complete intersection, the theory from [11] and [20] could also be used to study the codes $\mathrm{PRS}(N, \Delta_d)$ and their duals.

Corollary B.4.11. *Let $\Delta_d = \{0, 1, \ldots, d\}$ and $\Delta_{N-1-d} = \{0, 1, \ldots, N-1-d\}$. If $p \mid N$, then we have that $\mathrm{PRS}(N, \Delta_d)^\perp = \mathrm{PRS}(N, \Delta_{N-1-d})$.*

Proof. We can consider the monomials in (B.4.1), homogenizing up to degree $N - 1 - d$ with the variable x_0. Taking into account that in this case $\Delta^\perp \cup \{N - 1 - d\} = \Delta_{N-1-d}$ we obtain the result. □

With the evaluation map ev_{X_N}, if we consider the trace function $T : S \to S$, defined by $f \to f + f^q + \cdots + f^{q^{s-1}}$, then it is easy to verify that $\mathrm{ev}_{X_N} \circ T = \mathrm{Tr} \circ \mathrm{ev}_{X_N}$ (Tr was defined in Theorem B.4.1). Then we see that if $\mathrm{PRS}(N,\Delta)^\perp = \mathrm{ev}_{X_N}(\langle\{f_1, f_2, \ldots, f_l\}\rangle)$, using Theorem B.4.1 and the previous observation we get that

$$\begin{aligned}(\mathrm{PRS}(N,\Delta)_q)^\perp :=& (\mathrm{PRS}(N,\Delta)_q)^\perp \\ &= \mathrm{Tr}(\mathrm{ev}_{X_N}(\langle\{f_1, f_2, \ldots, f_l\}\rangle)) = \mathrm{ev}_{X_N}(T(\langle\{f_1, f_2, \ldots, f_l\}\rangle)).\end{aligned}$$

Remark B.4.12. Taking into account that T is linear, then it is clear that in this situation $(\mathrm{PRS}(N,\Delta)_q)^\perp$ is spanned by the image by the evaluation of the polynomials $T(\gamma f_i)$, $\gamma \in \mathbb{F}_{q^s}$, $i = 1, \ldots, l$.

Even if f_i, for $i = 1, \ldots, l$, are monomials, the dual code will be generated by traces of those monomials by Remark B.4.12, which in general are going to be non-homogeneous polynomials. We have introduced the vanishing ideal from Proposition B.4.6 precisely to understand linear independence of sets of monomials of different degree over X_N. In order to state a basis for $(\mathrm{PRS}(N,\Delta)_q)^\perp$ we will need the following lemma.

Lemma B.4.13. *Let $\Delta \subset \{0, 1, \ldots, N-1\}$ and $0 < a \neq N-1$. Then we have that $\mathfrak{I}_a \subset \Delta \iff \left|\mathfrak{I}_{N-1-a} \cap \Delta^\perp\right| = 0$.*

Proof. It is clear that we have a bijection between $\mathfrak{I}_a$ and $\mathfrak{I}_{-a}$, given by $h \mapsto -h$. In $\mathbb{Z}_N$ we have that $-h \equiv N-1-h \mod N-1$ if $h \neq 0$. Hence, we get a bijection between $\mathfrak{I}_a$ and $\mathfrak{I}_{N-1-a}$ given by $h \mapsto N-1-h$. Because of the definition of $\Delta^\perp$, we see that if $h \in \Delta$, then $N-1-h \notin \Delta^\perp$. Thus, it is clear that if $\mathfrak{I}_a \subset \Delta$, then $\left|\mathfrak{I}_{N-1-a} \cap \Delta^\perp\right| = 0$, and vice versa. □

Theorem B.4.14. *Let Δ be a nonempty subset of $\{0, 1, \ldots, N-1\}$ and let $d = d(\Delta)$. Set ξ_a a primitive element of the field $\mathbb{F}_{q^{n_a}}$ with $\mathcal{T}_a(\xi_a) \neq 0$ (this can always be done [8]). A basis for $(\mathrm{PRS}(N,\Delta)_q)^\perp$ is given by the image by ev_{X_N} of the following polynomials.*

If $\mathfrak{I}_d \subset \Delta$:

$$\bigcup_{a \in \mathcal{A} \mid \mathfrak{I}_a \cap \Delta^\perp \neq \emptyset} \{\mathcal{T}_a(\xi_a^r x_0 x_1^a) \mid 0 \leq r \leq n_a - 1\} \cup \{\mathcal{T}_{N-1-d}(\xi_{N-1-d}^r x_1^{N-1-d}) \mid 0 \leq r \leq n_{N-1-d} - 1\}.$$

If $\mathfrak{I}_d \not\subset \Delta$:

$$\bigcup_{a \in \mathcal{A} \mid \mathfrak{I}_a \cap \Delta^\perp \neq \emptyset} \{\mathcal{T}_a(\xi_a^r x_0 x_1^a) \mid 0 \leq r \leq n_a - 1\} \cup \{\mathcal{T}_{N-1-d}(\xi_{N-1-d} x_1^{N-1-d})\}.$$

Proof. In Remark B.4.12 we saw that it is enough to consider the traces of multiples of the monomials whose images span $\mathrm{PRS}(N,\Delta)^\perp$. Therefore, we have that the traces of multiples of the monomials in (B.4.1) span $\mathrm{Tr}(\mathrm{PRS}(N,\Delta)^\perp) = (\mathrm{PRS}(N,\Delta)_q)^\perp$. Moreover, it is enough to consider the following traces for $\mathfrak{I}_a$ with $\mathfrak{I}_a \cap \Delta^\perp \neq \emptyset$

$$\{\mathcal{T}_a(\xi_a^r x_0 x_1^a), 0 \leq r \leq n_a - 1\}$$

because they are linearly independent (a dependence relation would give a polynomial relation on ξ_a of degree less than n_a) and there are n_a of them, which is the maximum

dimension that we can get with n_a monomials. The same reasoning shows that it is enough to consider the following traces for the monomial x_1^{N-1-d}:

$$\{\mathcal{T}_{N-1-d}(\xi_{N-1-d}^r x_1^{N-1-d}), 0 \leq r \leq n_{N-1-d} - 1\}, \tag{B.4.4}$$

which are linearly independent between them as well.

If $\mathfrak{I}_d \subset \Delta$, by Lemma B.4.13 we have that $\left|\mathfrak{I}_{N-1-d} \cap \Delta^\perp\right| = \emptyset$. Hence, when we consider all of these sets of polynomials together, they are independent because between sets corresponding to different cyclotomic sets $\mathfrak{I}_a$ we have polynomials with disjoint support (the monomials that we are considering are linearly independent in $S/I(X_N)$ by Corollary B.4.9).

On the other hand, when $\mathfrak{I}_d \not\subset \Delta$, by Lemma B.4.13 we know that there is at least one element $h \in \mathfrak{I}_{N-1-d} \cap \Delta^\perp$. The argument for the previous case works in this case, except when considering the traces of polynomials associated to $\mathfrak{I}_{N-1-d}$ and the polynomials in (B.4.4), because by Lemma B.4.8 we will have the same powers of x_1. However, if from the later set of polynomials we only consider $\mathcal{T}_{N-1-d}(\xi_{N-1-d}x_1^{N-1-d})$, then the linear independence is clear because this polynomial is equal to $\mathcal{T}_{N-1-d}(\xi_{N-1-d}) \neq 0$ at $[0:1]$ (because of the choice of the primitive elements), while the rest of polynomials that we are considering are 0 at $[0:1]$. Moreover, with these polynomials we can generate the rest of the polynomials in (B.4.4) taking into account Lemma B.4.8:

$$\begin{aligned}\mathcal{T}_a(\xi_a^r x_0 x_1^a) =& \xi_a^r(x_0 + x_1^a - 1) + \xi_a^{qr}(x_0 + x_1^{qa} - 1) + \cdots + \xi_a^{q^{n_a-1}r}(x_0 + x_1^{q^{n_a-1}a} - 1) = \\ & \mathcal{T}_a(\xi_a^r)(x_0 - 1) + \mathcal{T}_a(\xi_a^r x_1^a).\end{aligned}$$

With $r = 1$ we see that we can generate $(x_0 - 1)$ with the polynomials we are considering, and with $(x_0 - 1)$ we can generate the rest of polynomials in (B.4.4) because $\mathcal{T}_a(\xi_a^r) \in \mathbb{F}_q$. □

In the case $\mathfrak{I}_{d(\Delta)} \not\subset \Delta$ of the previous result, we have seen that we can generate $(x_0 - 1)$. The evaluation of this polynomial on P^1 gives a codeword with Hamming weight 1, which means that $(\mathrm{PRS}(N, \Delta)_q)^\perp$ has minimum distance 1. This is equivalent to having that $\mathrm{PRS}(N, \Delta)_q$ is a degenerate code (it has a common zero in the coordinate associated to the point $[0:1]$). Once again, we see that the interesting case for us is when $\mathfrak{I}_{d(\Delta)} \subset \Delta$.

Example B.4.15. We continue with example B.3.2. Let $\Delta_4 = \{0, 1, 2, 3, 4\}$, which implies $d(\Delta_4) = 4$. We are going to obtain a set of polynomials such that its image by the evaluation map is a basis for $(\mathrm{PRS}(9, \Delta_4)_3)^\perp$. We have that $\Delta_4^\perp = \{0, 1, 2, 3\}$. The minimal cyclotomic sets $\mathfrak{I}_a$ with $\mathfrak{I}_a \cap \Delta^\perp \neq \emptyset$ are $\mathfrak{I}_0, \mathfrak{I}_1$ and $\mathfrak{I}_2$. As in the previous examples, if ξ is a primitive element of $\mathbb{F}_9$, by Theorem B.4.14, we obtain the following set of polynomials:

$$\begin{gathered}\mathcal{T}_0(x_0) = x_0, \mathcal{T}_1(x_0x_1) = x_0x_1 + x_0^3x_1^3, \mathcal{T}_1(\xi x_0x_1) = \xi x_0x_1 + \xi x_0^3x_1^3 \\ \mathcal{T}_2(x_0x_1^2) = x_0x_1^2 + x_0^3x_1^6, \mathcal{T}_2(\xi x_0x_1^2) = \xi x_0x_1^2 + \xi^3x_0^3x_1^6, \mathcal{T}_4(x_1^4) = x_1^4.\end{gathered}$$

In all the previous expressions, we can reduce the exponent of x_0 to 1 and the evaluation would not change.

As a consequence of Theorem B.4.14, we obtain directly an explicit formula for the dimension of $(\mathrm{PRS}(N,\Delta)_q)^\perp$ without using the dimension of the primary codes from Corollary B.3.7.

Corollary B.4.16. *Let $\Delta \subset \{0,1,\dots,N-1\}$ and let $d = d(\Delta)$. The dimension of $(\mathrm{PRS}(N,\Delta)_q)^\perp$ is equal to:*

$$\dim\left(\mathrm{PRS}(N,\Delta)_q\right)^\perp = \begin{cases} \displaystyle\sum_{a\in\mathcal{A}|\mathfrak{I}_a\cap\Delta^\perp\neq\emptyset} n_a + n_d & \text{if } \mathfrak{I}_d \subset \Delta \\ \displaystyle\sum_{a\in\mathcal{A}|\mathfrak{I}_a\cap\Delta^\perp\neq\emptyset} n_a + 1 & \text{if } \mathfrak{I}_d \not\subset \Delta \end{cases}$$

Now we are going to turn our attention to the minimum distance of the dual code $(\mathrm{PRS}(N,\Delta)_q)^\perp$. In the affine case, a BCH-type bound has been used frequently for the minimum distance of the duals of the subfield subcodes of Reed-Solomon codes. If one considers the code $\mathrm{RS}(N,\Delta)$ with $\Delta = \mathfrak{I}_{a_0}\cup\mathfrak{I}_{a_1}\cup\cdots\cup\mathfrak{I}_{a_l}$ a union of cyclotomic sets, then this code is Galois invariant in the sense of [2], i.e., $\mathrm{RS}(N,\Delta) = (\mathrm{RS}(N,\Delta))^q$. By [2, Thm. 4], we have that $\mathrm{Tr}(\mathrm{RS}(N,\Delta)) = \mathrm{RS}(N,\Delta)_q$. We can write Theorem B.4.1 in the following way: $C^\perp \cap \mathbb{F}_q^n = \mathrm{Tr}(C)^\perp$. Therefore, we have that $(\mathrm{RS}(N,\Delta)_q)^\perp = \left(\mathrm{RS}(N,\Delta)^\perp\right)_q$. For $(\mathrm{RS}(N,\Delta)^\perp)_q$, it is easy to see that we have a BCH-type bound because we can consider the generator matrix of $\mathrm{RS}(N,\Delta)$ as a pseudo-parity check matrix for the code $(\mathrm{RS}(N,\Delta)^\perp)_q$ (as we did with the matrix in (B.2.1) for BCH codes). If we have t consecutive exponents in Δ, we have a Vandermonde matrix as a submatrix of the generator matrix for $\mathrm{RS}(N,\Delta)$ and we get that $\mathrm{wt}\left((\mathrm{RS}(N,\Delta)_q)^\perp\right) \geq t+1$.

In the projective case, arguing in a similar way, we get that, if we have t consecutive exponents in Δ, we have the BCH-type bound $\mathrm{wt}\left((\mathrm{PRS}(N,\Delta)^\perp)_q\right) \geq t+1$. However, even if Δ is a union of cyclotomic sets, we will see in Remark B.4.23 and Example B.4.24 that in the projective case we do not have in general that $\mathrm{PRS}(N,\Delta)$ is Galois invariant, and thus we do not have the equality between $(\mathrm{PRS}(N,\Delta)^\perp)_q$ and $(\mathrm{PRS}(N,\Delta)_q)^\perp$ in general. Nevertheless, we can still use the affine case in order to get a bound for the minimum distance. If we have a code $C \subset \mathbb{F}_q^n$, we are going to denote by $(C,0) := \{(u_1,\dots,u_n,0) \in \mathbb{F}_q^{n+1} \mid u = (u_1,\dots,u_n) \in C\}$. In what follows, we are going to assume that the coordinate associated to the point $[0:1]$ is the last one. We recall that $\mathcal{A}$ (resp. $\mathcal{B}$) is the set of minimal representatives (resp. maximal representatives) of the minimal cyclotomic sets. We are going to denote $\Delta' := \Delta \setminus \{d\}$, and $(\Delta')_\mathfrak{I} = \bigcup_{b\in\mathcal{B},b<d|\mathfrak{I}_b\subset\Delta} \mathfrak{I}_b \subset \Delta'$ as before.

Proposition B.4.17. *Let $\Delta \subset \{0,1,\dots,N-1\}$. We assume that $d(\Delta) \in \mathcal{B}$ with $\mathfrak{I}_{d(\Delta)} \subset \Delta$. If t is the number of consecutive exponents in $(\Delta')_\mathfrak{I}$, then we have that $\mathrm{wt}\left((\mathrm{PRS}(N,\Delta)_q)^\perp\right) \geq t+1$.*

Proof. We assume that the point $[0:1]$ corresponds to the last coordinate. We have $\mathrm{PRS}(N,\Delta)_q \supset (\mathrm{RS}(N,\Delta')_q, 0)$, which implies

$$(\mathrm{PRS}(N,\Delta)_q)^\perp \subset (\mathrm{RS}(N,\Delta')_q,0)^\perp = ((\mathrm{RS}(N,\Delta')_q)^\perp,0) + \langle(0,\dots,0,1)\rangle.$$

We know that $(0,\dots,0,1) \notin (\mathrm{PRS}(N,\Delta)_q)^\perp$ because that would imply that $\mathrm{PRS}(N,\Delta)_q$ is degenerate, and that is not the case because of the assumptions that we have made. Thus, any vector in $(\mathrm{PRS}(N,\Delta)_q)^\perp$ must belong to $(\mathrm{RS}(N,\Delta')_q)^\perp$ after puncturing the last coordinate, and therefore the weight of any vector in $(\mathrm{PRS}(N,\Delta)_q)^\perp$ must be at least $t+1$ because of the BCH-type bound for $(\mathrm{RS}(N,\Delta')_q)^\perp$. □

As a corollary, we have the following result about the duals of the subfield subcodes of doubly extended Reed-Solomon codes.

Corollary B.4.18. *Let $\Delta_d = \{0, 1, \ldots, d\}$ with $d \in \mathcal{B}$. If t is the number of consecutive exponents in $(\Delta'_d)_{\mathfrak{J}}$, the parameters of $(\mathrm{PRS}(q^s, \Delta_d)_q)^\perp$ are $[q^s + 1, \sum_{a \in \mathcal{A} | \mathfrak{I}_a \cap \Delta^\perp \neq \emptyset} n_a, \geq t + 1]$.*

This estimate would give codes with length 1 more than in the affine case, but same dimension and same bound for the minimum distance. However, the bound for the minimum distance is not sharp in general and we are able to improve upon the affine case in many examples. For instance, in the next result we show that when $|\mathfrak{I}_d| = 1$ we have a better estimate for the minimum distance.

Proposition B.4.19. *Let $\Delta \subset \{0, 1, \ldots, N-1\}$ such that $\left|\mathfrak{I}_{d(\Delta)}\right| = 1$. Then $\mathrm{PRS}(N, \Delta_{\mathfrak{J}})$ is Galois invariant, we have that $(\mathrm{PRS}(N, \Delta_{\mathfrak{J}})^\perp)_q = (\mathrm{PRS}(N, \Delta_{\mathfrak{J}})_q)^\perp = (\mathrm{PRS}(N, \Delta)_q)^\perp$, and, if there are t consecutive exponents in $\Delta_{\mathfrak{J}}$, the parameters of $(\mathrm{PRS}(N, \Delta)_q)^\perp$ are $[N + 1, \sum_{a \in \mathcal{A} | \mathfrak{I}_a \cap \Delta_{\mathfrak{J}}^\perp \neq \emptyset} n_a + 1, \geq t + 1]$.*

Proof. Let $d = d(\Delta)$. We have that $\mathrm{PRS}(N, \Delta_{\mathfrak{J}})$ is generated by the evaluation of monomials. Because of the fact that $\Delta_{\mathfrak{J}}$ is a union of cyclotomic sets, we can divide the monomials into sets corresponding to different minimal cyclotomic sets. For $a \neq d$ we have the monomials

$$\{x_0 x_1^\alpha \mid \alpha \in \mathfrak{I}_a \subset \Delta\}.$$

If we consider these monomials to the power of q, the set remains invariant in $S/I(P^1)$ because the exponents of x_1 are in a cyclotomic set, and the exponent of x_0 does not change the evaluation. For $\mathfrak{I}_d$ we have that $x_1^{q(N-1-d)} \equiv x_1^{N-1-d} \mod I(P^1)$ because $|\mathfrak{I}_d| = 1$. Therefore, the set of monomials is invariant under taking powers of q, which implies that $\mathrm{PRS}(N, \Delta_{\mathfrak{J}}) = (\mathrm{PRS}(N, \Delta_{\mathfrak{J}}))^q$. Because of the previous discussion, we have that being Galois invariant implies in this case that $(\mathrm{PRS}(N, \Delta_{\mathfrak{J}})^\perp)_q = (\mathrm{PRS}(N, \Delta_{\mathfrak{J}})_q)^\perp$. Taking into account that $\mathrm{PRS}(N, \Delta_{\mathfrak{J}})_q = \mathrm{PRS}(N, \Delta)_q$ because of Theorem B.3.4, the parameters are clear from Theorem B.4.14 and the BCH-type bound. □

In many situations, the previous result gives codes with higher length and dimension than in the affine case. Assuming the hypotheses of the previous result, the affine code with $(\mathrm{RS}(N, \Delta)_q)^\perp$ would have parameters $[N, \sum_{a \in \mathcal{A} | \mathfrak{I}_a \cap \Delta_{\mathfrak{J}}^\perp \neq \emptyset} n_a, \geq t + 1]$, meanwhile the projective code $(\mathrm{PRS}(N, \Delta)_q)^\perp$ would have parameters $[N + 1, \sum_{a \in \mathcal{A} | \mathfrak{I}_a \cap \Delta_{\mathfrak{J}}^\perp \neq \emptyset} n_a + 1, \geq t + 1]$.

These codes can also be compared to $(\mathrm{RS}(N, \Delta')_q)^\perp$, with $\Delta' = \Delta \setminus \{d(\Delta)\}$. Taking into account that $|\mathfrak{I}_d| = 1$, this code has parameters $[N, \sum_{a \in \mathcal{A} | \mathfrak{I}_a \cap \Delta_{\mathfrak{J}}^\perp \neq \emptyset} n_a + 1, \geq t' + 1]$, where t' is the number of consecutive exponents in Δ'. We see that this code has the same dimension as $(\mathrm{PRS}(N, \Delta)_q)^\perp$. However, the bound for the minimum distance is worse than the one for $(\mathrm{PRS}(N, \Delta)_q)^\perp$.

The following result shows many situations in which we can use Proposition B.4.19 besides the obvious case with $\Delta = \{0\}$.

Lemma B.4.20. *Let $q > 2$. If $d_\lambda := \lambda(N-1)/(q-1) \in \mathbb{N}$, for some λ, $1 \leq \lambda \leq q-1$, then $|I_{d_\lambda}| = 1$.*

Proof. We only have to observe that

$$\lambda\frac{N-1}{q-1}q - \lambda\frac{N-1}{q-1} = \lambda(N-1) \equiv 0 \mod N-1.$$

□

Remark B.4.21. If $q-1 \mid N-1$, then with the previous result we obtain $q-1$ cyclotomic sets with cardinality one besides $\mathfrak{I}_0$. For example, if $N = q^s$, then we directly have $q-1 \mid N-1$. However, that is not the only case. For example we can consider $q^s = 3^8$ and $N = 83$. In that situation it can be checked that $q-1 = 2 \mid 82 = N-1$, and we have that $|I_{41}| = 1$. In this situation, when we have $q-1 \mid N-1$, the previous result is actually a characterization of when we have $|I_d| = 1$:

$$\begin{aligned} |I_d| = 1 &\iff dq \equiv d \mod N-1 \iff d(q-1) = \lambda(N-1) = \lambda(q-1)\frac{N-1}{q-1} \\ &\iff d = \lambda\frac{N-1}{q-1}, \text{ for some } 1 \leq \lambda < q-1. \end{aligned}$$

Example B.4.22. We consider the field extension $\mathbb{F}_{16} \supset \mathbb{F}_4$, which gives the following minimal cyclotomic sets:

$$\begin{gathered} \mathfrak{I}_0 = \{0\}, \mathfrak{I}_1 = \{1,4\}, \mathfrak{I}_2 = \{2,8\}, \mathfrak{I}_3 = \{3,12\}, \mathfrak{I}_5 = \{5\}, \\ \mathfrak{I}_6 = \{6,9\}, \mathfrak{I}_7 = \{7,13\}, \mathfrak{I}_{10} = \{10\}, \mathfrak{I}_{11} = \{11,14\}, \mathfrak{I}_{15} = \{15\}. \end{gathered}$$

We see that we have $|\mathfrak{I}_{10}| = 1$. If we take $\Delta = \{0,1,4,10\} = \mathfrak{I}_0 \cup \mathfrak{I}_1 \cup \mathfrak{I}_{10}$, then $\Delta^\perp = \{0,1,\ldots,N-1\} \setminus \{\mathfrak{I}_{15} \cup \mathfrak{I}_{11} \cup \mathfrak{I}_5\}$ and we can use Corollary B.4.16 to compute the dimension. All the cyclotomic sets, besides $\mathfrak{I}_5$, $\mathfrak{I}_{11}$ and $\mathfrak{I}_{15}$, have nonzero intersection with $\Delta^\perp$, and we have $\mathfrak{I}_{d(\Delta)} = \mathfrak{I}_{10} \subset \Delta$. Hence, by Corollary B.4.16, $\dim(\mathrm{PRS}(N,\Delta)_q)^\perp = (n_0+n_1+n_2+n_3+n_6+n_7+n_{10})+n_{10} = 13$. For the minimum distance, we have $t = 2$ consecutive elements in $\Delta_\mathfrak{I} = \Delta$, which gives the following parameters for $(\mathrm{PRS}(N,\Delta)_q)^\perp$: $[17, 13, \geq 3]$.

We can do the same for $\Delta = \{0,1,2,4,8,10\} = \mathfrak{I}_0 \cup \mathfrak{I}_1 \cup \mathfrak{I}_2 \cup \mathfrak{I}_{10}$, and we obtain the parameters $[17, 11, \geq 4]$. The true parameters are $[17, 13, 3]$ and $[17, 11, 4]$, which lengthen the parameters of the affine case $[16, 12, 3]$ and $[16, 10, 4]$. We see that the bound for the minimum distance coincides with the real minimum distance in this case.

Remark B.4.23. If we do not assume in Proposition B.4.19 that $|\mathfrak{I}_d| = 1$, then, if $d = d(\Delta) \in \mathcal{B}$ and $\mathfrak{I}_d \subset \Delta$ (which is the interesting case in the projective setting), we will have the evaluation of the monomial x_1^d in $\mathrm{PRS}(N,\Delta)$, and also the evaluation of at least one monomial $x_0^{d-a}x_1^a$ with $a \in \mathfrak{I}_d \setminus \{d\}$. We know that $d \equiv q^r a \mod N-1$ for some $r > 0$. Thus, we have the image of $x_0^{d-q^{r-1}a}x_1^{q^{r-1}a}$ in $\mathrm{PRS}(N,\Delta)$, but if we take this monomial to the power of q, we get $x_0^{q(d-q^{r-1}a)}x_1^d \not\equiv x_1^d \mod I(P^1)$. It is not hard to check that we do not have the image of this monomial in $\mathrm{PRS}(N,\Delta)$, which implies that $\mathrm{PRS}(N,\Delta)$ is not Galois invariant. In the following example we show how this affects the bound for the minimum distance.

Example B.4.24. We continue with Example B.4.22. We can consider $\Delta = \{0,1,2,3,4\}$, which gives $\Delta_\mathfrak{I} = \mathfrak{I}_0 \cup \mathfrak{I}_1$. However, we do not have $|\mathfrak{I}_4| = 1$ and Proposition B.4.19 does

not hold in this case. For instance, there are $t = 2$ consecutive elements in Δ, but the parameters of $(\mathrm{PRS}(N, \Delta)_q)^\perp$ are $[17, 15, 2]$, and $2 < t + 1 = 3$. On the other hand, we have that $(\Delta')_\mathfrak{J} = \mathfrak{I}_0$, which only has $t = 1$ consecutive elements, and Proposition B.4.17 would give the parameters $[17, 15, \geq 2]$.

B.5 Applications to EAQECCs

This section is devoted to providing quantum codes from the linear codes developed in the previous section. Namely, we will construct EAQECCs using the CSS construction [15, Thm. 4] and the Hermitian construction [15, Thm. 3], as well as asymmetric EAQECCs [16].

B.5.1 Euclidean EAQECCs

In this section we will be interested in obtaining EAQECCs using the CSS construction [15, Thm. 4]. Given a nonempty set $U \subset \mathbb{F}_q^n$, we denote by $\mathrm{wt}(U)$ the number $\min\{\mathrm{wt}(v) \mid v \in U \setminus \{0\}\}$, extending the notation that we have been using only for linear codes until now.

Theorem B.5.1 (CSS Construction)**.** *Let $C_i \subset \mathbb{F}_q^n$ be linear codes of dimension k_i, for $i = 1, 2$. Then, there is an EAQECC with parameters $[[n, \kappa, \delta; c]]_q$, where*

$$c = k_1 - \dim(C_1 \cap C_2^\perp),\ \kappa = n - (k_1 + k_2) + c,\ \textit{and}$$
$$\delta = \min\left\{\mathrm{wt}\left(C_1^\perp \setminus \left(C_1^\perp \cap C_2\right)\right), \mathrm{wt}\left(C_2^\perp \setminus \left(C_2^\perp \cap C_1\right)\right)\right\}.$$

We are going to introduce some new notation for the codes we are going to use. In what follows, we are assuming that $p \mid N$.

Definition B.5.2. Let $\mathcal{A} = \{a_0 = 0 < a_1 < \cdots < a_j\}$, the set of minimal representatives of the minimal cyclotomic sets. We are going to consider a set $\Delta = \bigcup_{i=0}^{t-1} \mathfrak{I}_{a_i} \cup \{a_t\}$, i.e., the union of consecutive minimal cyclotomic sets with minimal representatives $a_0, \ldots, a_{t-1}$, and the minimal element a_t. For such a set Δ, we are going to consider the code $\mathcal{D}(N, \Delta)$ defined as the linear code generated by $\{\mathrm{ev}_{X_N}(x_0 x_1^\alpha) \mid \alpha \in \Delta \setminus \{a_t\}\} \cup \{\mathrm{ev}_{X_N}(x_1^{a_t})\}$.

Remark B.5.3. If we look at the basis for the dual codes from Proposition B.4.10, we see that $\mathcal{D}(N, \Delta) = \mathrm{PRS}(N, \Delta^*)^\perp$, with $\Delta^* = \{0, 1, \ldots, N-1\} \setminus \bigcup_{i=0}^{t-1} \mathfrak{I}_{N-1-a_i}$. In particular, the codes we are considering are not degenerate.

Although the previous remark shows that we can use the notation $\mathrm{PRS}(N, \Delta^*)^\perp$ instead of $\mathcal{D}(N, \Delta)$, in what follows we are going to use $\mathcal{D}(N, \Delta)$ because this will be the appropriate notation for Section B.6. This allows us to make reference to the following proofs directly from Section B.6, which helps to avoid repetition.

Remark B.5.4. By the definitions, it is clear that $\mathcal{D}(N, \Delta) = (\mathrm{RS}(N, \Delta'), 0) + \langle \mathrm{ev}_{X_N}(x_1^{a_t}) \rangle$, where $\Delta' = \Delta \setminus \{a_t\}$. This means that $\dim \mathcal{D}(N, \Delta) = \dim \mathrm{RS}(N, \Delta') + 1 = \dim \mathrm{RS}(N, \Delta)$. We also have that $\dim (\mathcal{D}(N, \Delta)^\perp)_q = \dim \mathrm{PRS}(N, \Delta^*)_q = N + 1 - \sum_{i=0}^{t} n_{a_i}$ from Corollary B.3.7. If $G_{N,\Delta}$ is a generator matrix of $\mathrm{RS}(N, \Delta)$, then we have that

$$\left(\begin{array}{c|c} & 0 \\ G_{N,\Delta} & \vdots \\ & 0 \\ \hline \mathrm{ev}_{Y_N}(x^{a_t}) & 1 \end{array}\right)$$

is a generator matrix of $\mathcal{D}(N,\Delta)$. We see that this does not correspond to any standard lengthening technique for linear codes. On the other hand, the BCH-type bound gives $\mathrm{wt}((\mathcal{D}(N,\Delta)^\perp)_q) \geq \mathrm{wt}(\mathcal{D}(N,\Delta)^\perp) \geq a_t + 2$.

Theorem B.5.5. *Let $\mathcal{A} = \{a_0 = 0 < a_1 < a_2 < \cdots < a_z\}$ be the set of minimal representatives of the cyclotomic sets $\mathfrak{J}_{a_i}$, $0 \leq i \leq z$, of $\{0,1,\ldots,N-1\}$ with respect to q. Let $\Delta = \bigcup_{i=0}^{t-1} \mathfrak{J}_{a_i} \cup \{a_t\}$ such that $\mathrm{RS}(N,\Delta'') \subset \mathrm{RS}(N,\Delta'')^\perp$, where $\Delta'' = \bigcup_{i=0}^{t} \mathfrak{J}_{a_i}$. Then we can construct an EAQECC with parameters $[[n,\kappa,\geq \delta; c]]_q$, where $n = N+1$, $\kappa = N + 1 - 2\left(\sum_{i=0}^{t} n_{a_i}\right) + c$, $\delta = a_t + 2$, and $c \leq 1$.*

Proof. We are going to consider the code $C_1 = C_2 = ((\mathcal{D}(N,\Delta)^\perp)_q)^\perp$ for the CSS Construction B.5.1. We have $\dim\left((\mathcal{D}(N,\Delta)^\perp)_q\right)^\perp = N + 1 - \dim\left(\mathcal{D}(N,\Delta)^\perp\right)_q = N + 1 - \dim \mathrm{PRS}(N,\Delta^*)_q = \sum_{i=0}^{t} n_{a_i}$ by Remark B.5.4. Remark B.5.4 also gives the lower bound $\mathrm{wt}((\mathcal{D}(N,\Delta)^\perp)_q) \geq a_t + 2$.

For the parameter c, we claim that

$$\dim\left((\mathcal{D}(N,\Delta)^\perp)_q \cap ((\mathcal{D}(N,\Delta)^\perp)_q)^\perp\right) \geq \dim(\mathrm{RS}(N,\Delta'')_q,0) - 1 = \sum_{i=0}^{t} n_{a_i} - 1,$$

which gives $c \leq 1$. Let $\Delta' = \Delta \backslash \{a_t\}$. By Remark B.5.4 we have $\mathcal{D}(N,\Delta) = (\mathrm{RS}(N,\Delta'),0) + \langle \mathrm{ev}_{X_N}(x_1^{a_t})\rangle$.

We consider $v \in (\mathrm{RS}(N,\Delta)^\perp,0)$. Then v is orthogonal to $(\mathrm{RS}(N,\Delta'),0)$ (taking into account that $\mathrm{RS}(N,\Delta') \subset \mathrm{RS}(N,\Delta)$), and it is also orthogonal to $\mathrm{ev}_{X_N}(x_1^{a_t})$ because the last coordinate of v is 0, which means that $v \cdot \mathrm{ev}_{X_N}(x_1^{a_t}) = v \cdot \mathrm{ev}_{X_N}(x_0 x_1^{a_t})$, and $\mathrm{ev}_{X_N}(x_0 x_1^{a_t}) \in (\mathrm{RS}(N,\Delta),0)$. Therefore, $v \in \mathcal{D}(N,\Delta)^\perp$. Taking into account the dimension and the fact that the codes $\mathcal{D}(N,\Delta)^\perp$ are not degenerate, we can write $\mathcal{D}(N,\Delta)^\perp = (\mathrm{RS}(N,\Delta)^\perp,0) + \langle w\rangle$, where w is a vector with a nonzero last entry.

We consider a basis for $(\mathcal{D}(N,\Delta)^\perp)_q$ now, and we can also assume that all the vectors in the basis, besides one vector w', have 0 as their last coordinate. Taking into account that $(\mathcal{D}(N,\Delta)^\perp)_q$ is not degenerate, this means that we have $(\mathcal{D}(N,\Delta)^\perp)_q = ((\mathrm{RS}(N,\Delta)^\perp)_q,0) + \langle w'\rangle$ for some vector w' with nonzero last coordinate. In this case we have $(\mathrm{RS}(N,\Delta)^\perp)_q = (\mathrm{RS}(N,\Delta'')^\perp)_q$ because $\Delta^\perp$ and $\Delta''^\perp$ contain the same complete minimal cyclotomic sets (which is what matters in order to compute the subfield subcode of the dual, this can be seen using Theorem B.2.2 and [14, Prop. 3]). Moreover, we have that $\mathrm{RS}(N,\Delta'')_q \subset (\mathrm{RS}(N,\Delta'')^\perp)_q = (\mathrm{RS}(N,\Delta'')_q)^\perp$ because this code is Galois invariant by the reasoning after Corollary B.4.16.

Thus, we have seen that $(\mathcal{D}(N,\Delta)^\perp)_q \supset ((\mathrm{RS}(N,\Delta'')^\perp)_q,0) \supset (\mathrm{RS}(N,\Delta'')_q,0)$. On the other hand, we have

$$((\mathcal{D}(N,\Delta)^\perp)_q)^\perp = \left((\mathrm{PRS}(N,\Delta'')_q,0) + \langle(0,0,\ldots,0,1)\rangle\right) \cap \langle w'\rangle^\perp.$$

Note that $(0,0,\ldots,0,1) \notin \langle w'\rangle^\perp$ because w' has a nonzero last coordinate. Hence, we can consider a basis for $((\mathcal{D}(N,\Delta)^\perp)_q)^\perp$ formed by $(\dim \mathrm{RS}(N,\Delta'')_q - 1)$ vectors $u_i \in (\mathrm{RS}(N,\Delta'')_q,0)$, and a vector w'' such that its last coordinate is nonzero. Note that not all vectors can have the last coordinate equal to 0 because that would mean that we have the vector $(0,0,\ldots,0,1) \in (\mathcal{D}(N,\Delta)^\perp)_q$, contradicting the bound given for the minimum distance. Therefore, all the vectors u_i are in $(\mathcal{D}(N,\Delta)^\perp)_q \cap ((\mathcal{D}(N,\Delta)^\perp)_q)^\perp$, which gives $c \leq 1$. □

Remark B.5.6. In [17], there are conditions in order to have $\mathrm{RS}(N, \Delta'') \subset \mathrm{RS}(N, \Delta'')^{\perp}$. For example, for the type of set Δ'' that we are considering in Theorem B.5.5, if, for every cyclotomic set $\mathfrak{I}_a \subset \Delta''$, we have $\mathfrak{I}_{N-1-a} \not\subset \Delta''$, then $\mathrm{RS}(N, \Delta'') \subset \mathrm{RS}(N, \Delta'')^{\perp}$.

For the code $\mathrm{RS}(N, \Delta'')^{\perp}$ we have the bound $\mathrm{wt}(\mathrm{RS}(N, \Delta'')^{\perp}) \geq a_{t+1} + 1$. However, we have $a_{t+1} + 1 = a_t + 2$ in many cases (this happens if and only if $a_t + 1 \notin \Delta''$, because in that case $a_{t+1} = a_t + 1$). In that situation, we have the same bound for the minimum distance for $\mathrm{RS}(N, \Delta'')^{\perp}$ and for the corresponding EAQECC from Theorem B.5.5. In the following discussion we will assume that $a_{t+1} + 1 = a_t + 2$.

If we get a QECC with parameters $[[n, \kappa, \delta; 0]]_q$ from the affine case using $\mathrm{RS}(N, \Delta'')_q$, then we would get an EAQECC with parameters $[[n + 1, \kappa + 1 + c, \delta; c]]_q$ in the projective case using Theorem B.5.5, where $c \leq 1$. If we take into account the rate $\rho := \kappa/n$ and the net rate $\overline{\rho} := (\kappa - c)/n$, we see that the code obtained with Theorem B.5.5 has better rate and net rate than the one obtained in the affine case. Moreover, it can be checked that the codes we obtain are not directly obtainable from the affine case using the propagation rules from [29], which can be adapted for EAQECCs arising from Theorem B.5.1 (for example, see [1]).

In the constructions from Theorem B.5.15 and Theorem B.6.6, the same argument shows that, as long as $a_{t+1} + 1 = a_t + 2$, we can obtain codes with better rates than the ones from the affine case, which cannot be deduced from the propagation rules from [29].

Example B.5.7. We consider $N = q^s = 3^4 = 81$, with $q = 3^2$ ($s = 2$). The first minimal cyclotomic sets, ordered by their minimal element, are

$$\mathfrak{I}_0 = \{0\},\ \mathfrak{I}_1 = \{1, 9\},\ \mathfrak{I}_2 = \{2, 18\},\ \mathfrak{I}_3 = \{3, 27\},\ \mathfrak{I}_4 = \{4, 36\},\ \mathfrak{I}_5 = \{5, 45\}.$$

With the notation that we have been using, we consider the minimal elements a_i, for $i = 0, \ldots, 5$, and $\Delta = \bigcup_{i=0}^{4} \mathfrak{I}_{a_i} \cup \{5\}$ ($t = 5$ with the previous notation). We have $\sum_{i=0}^{5} n_{a_i} = 11$, and we have $a_t + 2 = 7$. It is easy to check that $\mathfrak{I}_{N-1-a_i} \not\subset \Delta$ for $i = 0, \ldots, 5$. By Remark B.5.6 we have $\mathrm{RS}(N, \Delta'') \subset \mathrm{RS}(N, \Delta'')^{\perp}$ and we can apply Theorem B.5.5 in order to obtain a quantum code with parameters $[[82, 61, 7; 1]]_9$. If we had used the affine code $\mathrm{RS}(N, \Delta'')$ with $\Delta'' = \bigcup_{i=0}^{5} \mathfrak{I}_{a_i}$, the bound for the minimum distance would have been the same because $a_t + 1 = 8 \notin \Delta''$, and we would have obtained the code $[[81, 59, 7; 0]]_9$.

We can also get QECCs (EAQECCs with $c = 0$) directly under some assumptions, as the following result shows.

Proposition B.5.8. *Assume that $p > 2$. Let N be an odd integer such that $N - 1 \mid q^s - 1$ and $p \mid N$. We consider a union of cyclotomic sets $\Delta \subset \{0, 1, \ldots, N - 1\}$ such that $d = d(\Delta) = (N - 1)/2$. If t is the number of consecutive exponents in Δ, then we can construct a QECC with parameters $[[n, \kappa, \geq \delta; 0]]_q$, where $n = N + 1$, $\kappa = N + 1 - 2|\Delta|$, and $\delta = t + 1$.*

Proof. By Proposition B.4.19, Lemma B.4.20 and Remark B.5.3, we have that $\mathrm{PRS}(N, \Delta)$ is Galois invariant, and we have $\mathrm{wt}((\mathrm{PRS}(N, \Delta)_q)^{\perp}) \geq t + 1$. By Corollary B.4.11, if we consider $\Delta_d = \{0, 1, \ldots, (N - 1)/2\}$, we have that

$$\mathrm{PRS}(N, \Delta) \subset \mathrm{PRS}(N, \Delta_d) = \mathrm{PRS}(N, \Delta_d)^{\perp} \subset \mathrm{PRS}(N, \Delta)^{\perp}.$$

Therefore, considering the intersection with $\mathbb{F}_q^n$ we obtain $\mathrm{PRS}(N,\Delta)_q \subset (\mathrm{PRS}(N,\Delta)_q)^\perp$. If we consider $C_1 = C_2 = \mathrm{PRS}(N,\Delta)_q$ in the CSS Construction B.5.1, we have already obtained the length, the bound for the minimum distance, and $c = 0$, for the parameters of the corresponding quantum error-correcting code. For the dimension, we have $\dim \mathrm{PRS}(N,\Delta)_q = |\Delta|$ by Corollary B.3.7, taking into account that $|\mathfrak{I}_d| = 1$ in this case by Lemma B.4.20. □

Example B.5.9. We consider $q^s = 3^3$, $q = 3$ and $N = 3^3 = 27$. Let $\Delta = \mathfrak{I}_0 \cup \mathfrak{I}_1 \cup \mathfrak{I}_4 \cup \mathfrak{I}_{13}$ (note that $13 = (N-1)/2$). We are not considering consecutive cyclotomic sets, which means that the BCH-type bound for the minimum distance might not be accurate. Hence, we have computed it directly with Magma [5]. The code $(\mathrm{PRS}(N,\Delta)_q)^\perp$ has parameters $[28, 20, 6]$, which gives a QECC with parameters $[[28, 12, 6; 0]]_3$ by Proposition B.5.8, which are the best known parameters for a quantum code over $\mathbb{F}_3$ with that length and dimension according to [21]. With $\mathrm{RS}(N,\Delta)$ and $\mathrm{RS}(N,\Delta')$ (where $\Delta' = \Delta \setminus \{(N-1)/2\}$), we obtain the parameters $[27, 19, 6]$ and $[27, 20, 5]$ for the dual codes of their subfield subcodes, respectively. These codes would give QECCs with parameters $[[27, 11, 6; 0]]_3$ and $[[27, 13, 5; 0]]_3$, respectively, applying the CSS Construction B.5.1.

B.5.2 Asymmetric EAQECCs

As we said in the introduction, phase-shift and qudit-flip errors are not equally likely to occur. It is therefore desirable to obtain EAQECCs with different error correction capabilities for each of these types of errors. In order to construct asymmetric EAQECCs, we can use the following result from [16].

Theorem B.5.10. *Let $C_i \subset \mathbb{F}_q^n$ be linear codes of dimension k_i, for $i = 1, 2$. Then, there is an asymmetric EAQECC with parameters $[[n, \kappa, \delta_z/\delta_x; c]]_q$, where*

$$c = k_1 - \dim(C_1 \cap C_2^\perp),\ \kappa = n - (k_1 + k_2) + c,$$
$$\delta_z = \mathrm{wt}\left(C_1^\perp \setminus \left(C_1^\perp \cap C_2\right)\right) \text{ and } \delta_x = \mathrm{wt}\left(C_2^\perp \setminus \left(C_2^\perp \cap C_1\right)\right).$$

The two minimum distances δ_z and δ_x give the error correction capability of the corresponding asymmetric EAQECC, which can correct up to $\lfloor (\delta_z - 1)/2 \rfloor$ phase-shift errors and $\lfloor (\delta_x - 1)/2 \rfloor$ qudit-flip errors.

In sections B.3 and B.4 we obtained bases for both the primary codes $\mathrm{PRS}(N,\Delta)_q$ and their duals $(\mathrm{PRS}(N,\Delta)_q)^\perp$. This is the key for the proof of the following result, which allows us to construct asymmetric EAQECCs from subfield subcodes of projective Reed-Solomon codes. We recall that, for $\Delta \subset \{0, 1, \ldots, N-1\}$, we denote $\Delta_\mathfrak{I} = \bigcup_{\mathfrak{I}_a \subset \Delta} \mathfrak{I}_a$, and we also recall that $\mathcal{B}$ is the set of maximal representatives of the minimal cyclotomic sets.

Theorem B.5.11. *Let $1 \leq d_1, d_2 \leq N-1$, such that $d_i \in \mathcal{B}$, for $i = 1, 2$, and $p \mid N$. We consider $\Delta_{d_i} = \{0, 1, \ldots, d_i\}$ and we denote $\Delta'_{d_i} := \Delta_{d_i} \setminus \{d_i\}$, for $i = 1, 2$. If $((\Delta'_{d_1})_\mathfrak{I})^\perp \subset (\Delta'_{d_2})_\mathfrak{I}$, then we can construct an asymmetric EAQECC with parameters*

$$[[N+1, \sum_{b \in \mathcal{B}, b < d_1} n_b + \sum_{b \in \mathcal{B}, b < d_2} n_b + 2 - N, \delta_z/\delta_x; 1]]_q,$$

where $\delta_z \geq N - d_1 + 1$, $\delta_x \geq N - d_2 + 1$.

Proof. We are going to consider $C_i = (\mathrm{PRS}(N, \Delta_{d_i})_q)^\perp$, for $i = 1, 2$, and we are going to use Theorem B.5.10. The bounds for δ_z and δ_x are clear, and we obtain the dimension using Corollary B.3.7 if we assume $c = 1$. For the parameter $c = \dim(\mathrm{PRS}(N, \Delta_{d_1})_q)^\perp - \dim((\mathrm{PRS}(N, \Delta_{d_1})_q)^\perp \cap \mathrm{PRS}(N, \Delta_{d_2})_q)$, we are going to study $\dim((\mathrm{PRS}(N, \Delta_{d_1})_q)^\perp \cap \mathrm{PRS}(N, \Delta_{d_2})_q)$. For $(\mathrm{PRS}(N, \Delta_{d_1})_q)^\perp$ we have the basis given by the evaluation of the following set from Theorem B.4.14:

$$\bigcup_{a \in \mathcal{A} | \mathfrak{I}_a \cap \Delta_{d_1}^\perp \neq \emptyset} \{\mathcal{T}_a(\xi_a^r x_0 x_1^a) \mid 0 \leq r \leq n_a - 1\} \cup \{\mathcal{T}_{N-1-d_1}(\xi_{N-1-d_1}^r x_1^{N-1-d_1}) \mid 0 \leq r \leq n_{d_1} - 1\}. \tag{B.5.1}$$

From Theorem B.3.4 it is easy to obtain that the evaluation of the following set gives a basis for $\mathrm{PRS}(N, \Delta_{d_2})_q$:

$$\bigcup_{a \in \mathcal{A} | \mathfrak{I}_a \subset \Delta'_{d_2}} \{\mathcal{T}_a(\xi_a^r x_0 x_1^a) \mid 0 \leq r \leq n_a - 1\} \cup \{\mathcal{T}_{d_2}^h(x_1^{d_2})\}. \tag{B.5.2}$$

It is also clear that the $a \in \mathcal{A}$ such that $\mathfrak{I}_a \cap \Delta_{d_1}^\perp \neq \emptyset$ are precisely the $a \in \mathcal{A}$ such that $\mathfrak{I}_a \subset ((\Delta_{d_1})_\mathfrak{I})^\perp$. We also have that $((\Delta'_{d_1})_\mathfrak{I})^\perp = ((\Delta_{d_1})_\mathfrak{I})^\perp \cup \mathfrak{I}_{N-1-d_1}$. Therefore, taking into account the assumption $((\Delta'_{d_1})_\mathfrak{I})^\perp \subset (\Delta'_{d_2})_\mathfrak{I} \subset \Delta'_{d_2}$, we have that all the traces of monomials of the type $x_0 x_1^a$, with $a \in \mathcal{A}$, in the set from (B.5.1), are contained in the set from (B.5.2). This implies that the evaluation of the set

$$\bigcup_{a \in \mathcal{A} | \mathfrak{I}_a \cap \Delta_{d_1}^\perp \neq \emptyset} \{\mathcal{T}_a(\xi_a^r x_0 x_1^a) \mid 0 \leq r \leq n_a - 1\} \tag{B.5.3}$$

is in $(\mathrm{PRS}(N, \Delta_{d_1})_q)^\perp \cap \mathrm{PRS}(N, \Delta_{d_2})_q$.

Now we are going to study which polynomials from the set generated by

$$\{\mathcal{T}_{N-1-d_1}(\xi_{N-1-d_1}^r x_1^{N-1-d_1}) \mid 0 \leq r \leq n_{d_1} - 1\}$$

have their evaluation in $(\mathrm{PRS}(N, \Delta_{d_1})_q)^\perp \cap \mathrm{PRS}(N, \Delta_{d_2})_q$. As in Theorem B.4.14, we assume that ξ_{N-1-d_1} is a primitive element of $\mathbb{F}_{q^{n_{d_1}}}$ (note that $n_{d_1} = n_{N-1-d_1}$) such that $\mathcal{T}_{N-1-d_1}(\xi_{N-1-d_1}) \neq 0$. For ease of notation, we are going to denote now $d'_1 = N - 1 - d_1$. For $0 \leq r \leq n_{d_1} - 1$, $r \neq 1$, we have

$$\begin{aligned} &\mathcal{T}_{d'_1}(\xi_{d'_1})\mathcal{T}_{d'_1}(\xi_{d'_1}^r x_0 x_1^{d'_1}) - \mathcal{T}_{d'_1}(\xi_{d'_1}^r)\mathcal{T}_{d'_1}(\xi_{d'_1} x_0 x_1^{d'_1}) \\ &\qquad \equiv \mathcal{T}_{d'_1}(\xi_{d'_1})\mathcal{T}_{d'_1}(\xi_{d'_1}^r x_1^{d'_1}) - \mathcal{T}_{d'_1}(\xi_{d'_1}^r)\mathcal{T}_{d'_1}(\xi_{d'_1} x_1^{d'_1}) \bmod I(X_N). \end{aligned} \tag{B.5.4}$$

This is easy to see because when we set $x_0 = 1$, we obtain the same polynomials at each side, which means that they have the same evaluation in $[\{1\} \times Y_N]$, and both polynomials evaluate to 0 in $[0 : 1]$. Therefore, they have the same evaluation in X_N. Because of the assumption $((\Delta'_{d_1})_\mathfrak{I})^\perp = ((\Delta_{d_1})_\mathfrak{I})^\perp \cup \mathfrak{I}_{d'_1} \subset (\Delta'_{d_2})_\mathfrak{I}$, we obtain $\mathfrak{I}_{d'_1} \subset \Delta'_{d_2}$ and it is clear that we have the evaluation of the polynomial in the left-hand side of (B.5.4) in $\mathrm{PRS}(N, \Delta_{d_2})_q$ if we consider the basis from (B.5.2). The evaluation of the polynomial in the right-hand side is clearly in $(\mathrm{PRS}(N, \Delta_{d_1})_q)^\perp$ (see (B.5.1)). Thus, we have proved that the image by the evaluation map of the polynomials in the set

$$\{\mathcal{T}_{d'_1}(\xi_{d'_1})\mathcal{T}_{d'_1}(\xi_{d'_1}^r x_0 x_1^{d'_1}) - \mathcal{T}_{d'_1}(\xi_{d'_1}^r)\mathcal{T}_{d'_1}(\xi_{d'_1} x_0 x_1^{d'_1}) \mid 0 \leq r \leq n_{d_1} - 1, r \neq 1\} \tag{B.5.5}$$

is in $(\mathrm{PRS}(N, \Delta_{d_1})_q)^\perp \cap \mathrm{PRS}(N, \Delta_{d_2})_q$.

Hence, the evaluation of the union of the sets from (B.5.3) and (B.5.5) is in

$$(\mathrm{PRS}(N, \Delta_{d_1})_q)^\perp \cap \mathrm{PRS}(N, \Delta_{d_2})_q,$$

and it is easy to see that the evaluation of this union is linearly independent. Taking into account the basis from (B.5.1), we obtain that $\dim((\mathrm{PRS}(N, \Delta_{d_1})_q)^\perp \cap \mathrm{PRS}(N, \Delta_{d_2})_q) \geq \dim((\mathrm{PRS}(N, \Delta_{d_1})_q)^\perp) - 1$, i.e., $c \leq 1$.

On the other hand, having $c = 0$ means that $(\mathrm{PRS}(N, \Delta_{d_1})_q)^\perp \subset \mathrm{PRS}(N, \Delta_{d_2})_q$. This implies that the evaluation of all the traces appearing in (B.5.4) are in $\mathrm{PRS}(N, \Delta_{d_2})_q$. However, the evaluations of $\mathcal{T}_{d'_1}(\xi_{d'_1} x_0 x_1^{d'_1})$ and $\mathcal{T}_{d'_1}(\xi_{d'_1} x_1^{d'_1})$ differ only at the coordinate associated to the point $[0 : 1]$. This would imply that the minimum distance of $\mathrm{PRS}(N, \Delta_{d_2})_q$ is 1, a contradiction. Therefore, $c = 1$. □

Remark B.5.12. We note that in the previous result we have that $(\Delta'_d)_{\mathfrak{I}} = \bigcup_{b \in \mathcal{B} | b < d} \mathfrak{I}_b$.

As we said in the introduction, it is desirable to obtain asymmetric quantum codes with higher error-correction capability for phase-shift errors, i.e. with $\delta_z > \delta_x$. For the codes obtained using Theorem B.5.11, this corresponds to choosing $d_1 < d_2$.

In the next example we show that we are able to obtain codes which are better than the ones available in the current literature.

Example B.5.13. We consider the extension $\mathbb{F}_{16} \supset \mathbb{F}_4$, which is the setting from Example B.4.22. We choose $d_1 = 14$, $d_2 = 15$, and apply Theorem B.5.11, which gives the parameters $[[17, 14, 3/2; 1]]_4$. In [16], we can find a code with parameters $[[15, 12, 3/2; 1]]_4$ using BCH codes. We see that the code we have obtained has better rate κ/n, and also better net rate $(\kappa - c)/n$.

If we consider the extension $\mathbb{F}_{25} \supset \mathbb{F}_5$ instead, and choose $d_1 = 22$, $d_2 = 23$, we obtain a code with parameters $[[26, 19, 4/3; 1]]_5$ using Theorem B.5.11. It is possible to adapt the propagation rules from [29] to asymmetric EAQECCs arising from Theorem B.5.10. For example, we can reduce the length by using extra entanglement, provided that $c \leq n - \kappa - 2$:

$$[[n, \kappa, \delta_z/\delta_x; c]]_q \to [[n - 1, \kappa, \delta_z/\delta_x; c + 1]]_q. \tag{B.5.6}$$

In [16] a code with parameters $[[24, 19, 4/3; 3]]_5$ is presented, which can be obtained from our code with parameters $[[26, 19, 4/3; 1]]_5$ by applying (B.5.6) two times. In this sense, we can say that the parameters $[[24, 19, 4/3; 3]]_5$ appearing in [16] are a consequence of the parameters $[[26, 19, 4/3; 1]]_5$ that we obtain with Theorem B.5.11.

Finally, if we consider the extension $\mathbb{F}_{64} \supset \mathbb{F}_8$, for $d_1 = 60$ and $d_2 = 63$, we obtain the parameters $[[65, 58, 5/2; 1]]_8$, which give a better rate and net rate than the code with parameters $[[63, 56, 5/2; 1]]_8$ from [16]. If we choose $d_1 = 58$ and $d_2 = 62$ instead, we obtain the parameters $[[65, 52, 7/3; 1]]_8$, which, after using the propagation rule (B.5.6) as before, give the parameters $[[63, 52, 7/3; 3]]_8$ that appear in [16].

If we do not assume $((\Delta'_{d_1})_{\mathfrak{I}})^\perp \subset (\Delta'_{d_2})_{\mathfrak{I}}$ in Theorem B.5.11, then we would obtain instead the parameters $[[N + 1, \sum_{b \in \mathcal{B}, b < d_1} n_b + \sum_{b \in \mathcal{B}, b < d_2} n_b + 1 + c - N, \delta_z/\delta_x; c]]_q$, for $c = \dim(\mathrm{PRS}(N, \Delta_{d_1})_q)^\perp - \dim((\mathrm{PRS}(N, \Delta_{d_1})_q)^\perp \cap \mathrm{PRS}(N, \Delta_{d_2})_q)$.

B.5.3 Hermitian EAQECCs

In the Hermitian case, we have to work with three different fields. Hence, we are going to change the notation from the previous sections. We consider the field extension $\mathbb{F}_{q^{2\ell}} \supset \mathbb{F}_{q^2}$, where $q^{2\ell} = p^{2r}$, $q = p^s$, for some $r, s > 0$, and $r = \ell s$. Thus, in what follows we are going to obtain codes of length $n = N + 1$, where $N > 1$ is an integer such that $N - 1 \mid q^{2\ell} - 1$.

As before, we are going to consider the set $\mathbb{Z}_N = \{0\} \cup \{1, 2, \ldots, N-1\}$, where $\{1, 2, \ldots, N-1\}$ is regarded as the set of representatives of the ring $\mathbb{Z}/(N-1)\mathbb{Z}$. We consider the cyclotomic sets with respect to q^2 over $\{0, 1, \ldots, N-1\}$. We call $\mathcal{A}$ the set of minimal elements of the different cyclotomic sets. We introduce now the Hermitian construction [15, Thm. 3] that we are going to use.

Theorem B.5.14 (Hermitian construction)**.** *Let $C \subset \mathbb{F}_{q^2}^n$ be a linear code of dimension k and $C^{\perp_h}$ its Hermitian dual. Then, there is an EAQECC with parameters $[[n, \kappa, \delta; c]]_q$, where*

$$c = k - \dim(C \cap C^{\perp_h}),\ \kappa = n - 2k + c, \quad \textit{and} \quad \delta = \mathrm{wt}(C^{\perp_h} \setminus (C \cap C^{\perp_h})).$$

We are only going to consider the Hermitian product over $\mathbb{F}_{q^2}$. Therefore, for $a, b \in \mathbb{F}_{q^2}^n$ we have

$$a \cdot_h b := \sum_{i=0}^{n} a_i b_i^q.$$

In what follows, when considering a power of a code or a vector, we will be considering the component-wise power, i.e., $C^q := \{c^q := (c_1^q, \ldots, c_n^q) \mid c = (c_1, \ldots, c_n) \in C\}$. It is easy to check that, for codes over $\mathbb{F}_{q^2}$, we have that $C^\perp = (C^{\perp_h})^q$, where $C^{\perp_h}$ denotes the Hermitian dual.

Theorem B.5.15. *Let $\mathcal{A} = \{a_0 = 0 < a_1 < a_2 < \cdots < a_z\}$ be the set of minimal representatives of the cyclotomic sets $\mathfrak{I}_{a_i}$, $0 \le i \le z$, of $\{0, 1, \ldots, N-1\}$ with respect to q^2. Let $\Delta = \bigcup_{i=0}^{t-1} \mathfrak{I}_{a_i} \cup \{a_t\}$ such that $\mathrm{RS}(N, \Delta'')_{q^2} \subset (\mathrm{RS}(N, \Delta'')_{q^2})^{\perp_h}$, where $\Delta'' = \bigcup_{i=0}^{t} \mathfrak{I}_{a_i}$. Then we can construct an EAQECC with parameters $[[n, \kappa, \geq \delta; c]]_q$, where $n = N + 1$, $\kappa = N + 1 - 2\left(\sum_{i=0}^{t} n_{a_i}\right) + c$, $\delta = a_t + 2$ and $c \le 1$.*

Proof. We are going to consider the code $C = ((\mathcal{D}(N, \Delta)^\perp)_{q^2})^{\perp_h}$ for the Hermitian construction B.5.14. Using what we obtained in Theorem B.5.5, the only thing left to prove is the statement about the parameter c.

Following the proof of Theorem B.5.5, we have $(\mathcal{D}(N, \Delta)^\perp)_{q^2} = ((\mathrm{RS}(N, \Delta'')^\perp)_{q^2}, 0) + \langle w' \rangle$ for some vector w' with nonzero last coordinate. Therefore, $\dim((\mathcal{D}(N, \Delta)^\perp)_{q^2})^{\perp_h} = \dim \mathrm{RS}(N, \Delta'')_{q^2} = \dim((\mathrm{RS}(N, \Delta'')^\perp)_{q^2})^{\perp_h}$. Moreover, we have

$$((\mathrm{RS}(N, \Delta'')^\perp)_{q^2})^{\perp_h} = ((\mathrm{RS}(N, \Delta'')_{q^2})^\perp)^{\perp_h} = (((\mathrm{RS}(N, \Delta'')_{q^2})^\perp)^\perp)^q = \left(\mathrm{RS}(N, \Delta'')_{q^2}\right)^q.$$

Thus, we obtain

$$((\mathcal{D}(N, \Delta)^\perp)_{q^2})^{\perp_h} = (((\mathrm{PRS}(N, \Delta'')_{q^2})^q, 0) + \langle (0, 0, \ldots, 0, 1) \rangle) \cap \langle (w') \rangle^{\perp_h}.$$

Note that $(0, 0, \ldots, 0, 1) \notin \langle (w') \rangle^{\perp_h}$ because w' has a nonzero last coordinate. We can consider a basis for $((\mathcal{D}(N, \Delta)^\perp)_{q^2})^{\perp_h}$ formed by $(\dim \mathrm{RS}(N, \Delta'')_{q^2} - 1)$ vectors $u_i \in ((\mathrm{RS}(N, \Delta'')_{q^2})^q, 0)$, and a vector w such that its last coordinate is nonzero (not all vectors

can have the last coordinate equal to 0 because that would mean that we have the vector $(0,0,\ldots,0,1) \in (\mathcal{D}(N,\Delta)^{\perp})_{q^2}$, contradicting the bound given for the minimum distance).

By our hypothesis, we have $\mathrm{RS}(N,\Delta'')_{q^2} \subset (\mathrm{RS}(N,\Delta'')_{q^2})^{\perp_h}$. Thus, $\left(\mathrm{RS}(N,\Delta'')_{q^2}\right)^q \subset \left((\mathrm{RS}(N,\Delta'')_{q^2})^{\perp_h}\right)^q = (\mathrm{RS}(N,\Delta'')_{q^2})^{\perp} = (\mathrm{RS}(N,\Delta'')^{\perp})_{q^2}$. Taking into account that $(\mathcal{D}(N,\Delta)^{\perp})_{q^2} \supset ((\mathrm{RS}(N,\Delta'')^{\perp})_{q^2},0) \supset ((\mathrm{RS}(N,\Delta'')_{q^2})^q,0)$, we see that the vectors u_i are in $(\mathcal{D}(N,\Delta)^{\perp})_{q^2}$ as well, and we obtain the desired inequality for the dimension of the intersection. □

Remark B.5.16. From [17, Prop. 3] we can obtain conditions to have $\mathrm{RS}(N,\Delta'')_{q^2} \subset (\mathrm{RS}(N,\Delta'')_{q^2})^{\perp_h}$, like the one we show next. Let $\Delta'' = \bigcup_{i=0}^{t} \mathfrak{I}_{a_i}$, and we denote by a_i' the minimal element in $\mathcal{A}$ such that $\mathfrak{I}_{a_i'} = \mathfrak{I}_{-qa_i}$. Assuming $d(\Delta) < N-1$, if $\Delta'' \subset (\Delta'')^{\perp_h} := \{0,1,\ldots,N-1\} \setminus \bigcup_{i=0}^{t} \mathfrak{I}_{a_i'}$, then we have $\mathrm{RS}(N,\Delta'')_{q^2} \subset (\mathrm{RS}(N,\Delta'')_{q^2})^{\perp_h}$.

Example B.5.17. We continue with the setting from Example B.5.7. It is easy to check that the set Δ in Example B.5.7 satisfies $\Delta \subset \Delta^{\perp_h}$, and by Remark B.5.16 and Theorem B.5.15 we obtain a quantum code with parameters $[[82,67,7;1]]_3$.

With the construction from Theorem B.5.15 we can obtain several quantum codes over $\mathbb{F}_2$ whose parameters do not appear in the table of EAQECCs from [21], and therefore we improve the table. With the extension $\mathbb{F}_{2^4} \supset \mathbb{F}_{2^2}$, we can obtain a code with parameters $[[17,12,3;1]]_2$, which is not in the table from [21]. We can consider now the following propagation rule from [29]: let C be an EAQECC with parameters $[[n,\kappa,\delta;c]]_q$ obtained from Theorem B.5.14 (for example, the codes from Theorem B.5.15). If $c \leq n-\kappa-2$, then we can reduce the length by using extra entanglement:

$$[[n,\kappa,\delta;c]]_q \to [[n-1,\kappa,\delta;c+1]]_q. \tag{B.5.7}$$

Iterating this rule, it is easy to check that, from an EAQECC with parameters $[[n,\kappa,\delta;c]]_q$, one can obtain EAQECCs with parameters $[[n-s,\kappa,\delta;c+s]]_q$, $s=1,\ldots,(n-\kappa-c)/2$. Note that the maximum value for c is $k = \dim C$, where C is the classical code used for Theorem B.5.14, and for the maximum value of s that we have stated we have precisely that $c+s=k$:

$$c+s = c+\frac{n-\kappa-c}{2} = c+\frac{2k-2c}{2} = k.$$

Applying the propagation rule (B.5.7) to the parameters $[[17,12,3;1]]_2$, we obtain $[[16,12,3;2]]_2$ and $[[15,12,3;3]]_2$, which are also missing in the table [21].

For the extension $\mathbb{F}_{2^6} \supset \mathbb{F}_{2^2}$, we obtain codes with length 65, which is greater than the current maximum length in [21] for EAQECCs over $\mathbb{F}_2$. Nevertheless, we can reduce the length with the propagation rule (B.5.7) and check if the corresponding parameters are in the table. A code with parameters $[[64,58,3;2]]_2$, whose parameters are missing in [21], is obtained from the code with parameters $[[65,58,3;1]]_2$ derived from Theorem B.5.15 using (B.5.7). Moreover, by applying the propagation rule (B.5.7) to the code with parameters $[[65,40,7;1]]_2$ deduced from Theorem B.5.15, we obtain codes with parameters $[[65-i,40,7;1+i]]_2$, for $i=1,2,\ldots,12$, whose parameters are also missing in [21].

In total, we obtain in this way 16 EAQECCs over $\mathbb{F}_2$ whose parameters are missing in [21].

The table of EAQECCs from [21] also covers codes over $\mathbb{F}_3$. However, the smaller length that we can achieve with Theorem B.5.15 over $\mathbb{F}_3$ would be $3^4+1 = 82$, much higher than

the current maximum length in the table from [21] for this case. For example, we obtain codes with parameters $[[82, 77, 3; 1]]_3$, $[[82, 73, 4; 1]]_3$, $[[82, 69, 5; 1]]_3$ and $[[82, 65, 6; 1]]_3$.

B.6 Evaluating at the trace roots

In this section, following the ideas from [18], we are going to consider evaluation codes over the roots of a suitable trace polynomial. In [18], the authors considered the trace polynomial over $\mathbb{F}_{q^{2\ell}}$ with respect to $\mathbb{F}_q$ defined as

$$\mathrm{Tr}^{\mathrm{s}}_{2\mathrm{r}}(x) = x + x^q + x^{q^2} + \cdots + x^{q^{2\ell-1}}.$$

Let $Y_{\mathrm{Tr}_\ell} = \{\alpha \in \mathbb{F}_{q^{2\ell}} \mid \mathrm{Tr}^{\mathrm{s}}_{2\mathrm{r}}(\alpha) = 0\}$. It is well known that $|Y_{\mathrm{Tr}_\ell}| = q^{2\ell-1}$. In [18], evaluation codes over the roots of the trace are defined, obtaining codes with length $q^{2\ell-1}$, and bounds for the dimension and minimum distance of these codes are found. In this section we are going to do a similar thing over the projective space, obtaining codes of length $q^{2\ell-1} + 1$.

Firstly, we need to define the finite set of projective points in which we are going to evaluate. In order to do this, we are simply going to add the point at infinity to the set of roots of the trace, i.e., we are going to consider the following set of points:

$$\mathbb{X}_{\mathrm{Tr}^{\mathrm{s}}_{2\mathrm{r}}} = \{[1 : \alpha] \mid \mathrm{Tr}^{\mathrm{s}}_{2\mathrm{r}}(\alpha) = 0\} \cup \{[0 : 1]\}.$$

It is clear from the definition that $\left|\mathbb{X}_{\mathrm{Tr}^{\mathrm{s}}_{2\mathrm{r}}}\right| = q^{2\ell-1} + 1$. Moreover, we can give this set as the zeroes of a square-free homogeneous polynomial. In the rest of this section, when we consider the homogenization f^h of a polynomial f, we are considering the standard homogenization (up to degree $\deg(f)$).

Proposition B.6.1. *The vanishing ideal of* $\mathbb{X}_{\mathrm{Tr}^{\mathrm{s}}_{2\mathrm{r}}}$ *is* $I(\mathbb{X}_{\mathrm{Tr}^{\mathrm{s}}_{2\mathrm{r}}}) = \langle x_0(\mathrm{Tr}^{\mathrm{s}}_{2\mathrm{r}}(x_1))^h \rangle$.

Proof. The generator of the ideal is a homogeneous polynomial. Therefore, we can just look at the set of representatives P^1 to check the zeroes of the ideal. It is clear that $[0 : 1] \in V(\langle x_0(\mathrm{Tr}^{\mathrm{s}}_{2\mathrm{r}}(x_1))^h \rangle)$. And it is also clear that if $[1 : \alpha]$ is a zero of $x_0(\mathrm{Tr}^{\mathrm{s}}_{2\mathrm{r}}(x_1))^h$, then α must be a root of $\mathrm{Tr}^{\mathrm{s}}_{2\mathrm{r}}(x)$. Thus, we have that $V(\langle x_0(\mathrm{Tr}^{\mathrm{s}}_{2\mathrm{r}}(x_1))^h \rangle) = \mathbb{X}_{\mathrm{Tr}^{\mathrm{s}}_{2\mathrm{r}}}$.

On the other hand, we have the decomposition

$$\mathrm{Tr}^{\mathrm{s}}_{2\mathrm{r}}(x) = \prod_{\alpha \in \mathbb{F}_{q^{2\ell}} | \mathrm{Tr}^{\mathrm{s}}_{2\mathrm{r}}(\alpha) = 0} (x - \alpha).$$

Homogenizing and multiplying by x_0 we get

$$x_0(\mathrm{Tr}^{\mathrm{s}}_{2\mathrm{r}}(x_1))^h = x_0 \prod_{\alpha \in \mathbb{F}_{q^{2\ell}} | \mathrm{Tr}^{\mathrm{s}}_{2\mathrm{r}}(\alpha) = 0} (x_1 - \alpha x_0).$$

Therefore, $x_0(\mathrm{Tr}^{\mathrm{s}}_{2\mathrm{r}}(x_1))^h$ is a square-free polynomial and $\langle x_0(\mathrm{Tr}^{\mathrm{s}}_{2\mathrm{r}}(x_1))^h \rangle$ is a radical ideal by [9, Prop. 9, Chapter 4, Section 2], which means that it is equal to $I(\mathbb{X}_{\mathrm{Tr}^{\mathrm{s}}_{2\mathrm{r}}})$. □

If we consider the set of standard representatives $X_{\mathrm{Tr}^{\mathrm{s}}_{2\mathrm{r}}}$ of $\mathbb{X}_{\mathrm{Tr}^{\mathrm{s}}_{2\mathrm{r}}}$, we obtain the following vanishing ideal.

Proposition B.6.2. *The vanishing ideal of* $X_{\mathrm{Tr}^{\mathrm{s}}_{2\mathrm{r}}}$ *is*

$$I(X_{\mathrm{Tr}^{\mathrm{s}}_{2\mathrm{r}}}) = \langle x_0^2 - x_0, x_1^{q^{2\ell}} - x_1, (x_0-1)(x_1-1), x_0\,\mathrm{Tr}(x_1)\rangle.$$

Proof. It is clear that any point of $X_{\mathrm{Tr}^{\mathrm{s}}_{2\mathrm{r}}}$ satisfies the equations. On the other hand, any point that satisfies this equations must have the first coordinate equal to 0 or 1 because of the first equation. If it is 0, then by the equation $(x_0-1)(x_1-1) \equiv 0 \bmod I(X_{\mathrm{Tr}^{\mathrm{s}}_{2\mathrm{r}}})$ we have that the last coordinate is equal to 1. If the first coordinate is 1, then the last equation implies that the last coordinate must be a zero of $\mathrm{Tr}(x)$. Therefore, $V(I(X_{\mathrm{Tr}^{\mathrm{s}}_{2\mathrm{r}}})) = X_{\mathrm{Tr}^{\mathrm{s}}_{2\mathrm{r}}}$. We obtain the result applying Seidenberg's Lemma [26, Prop. 3.7.15] and Hilbert's Nullstellensatz over the algebraic closure of $\mathbb{F}_{q^{2\ell}}$. □

We are going to define the evaluation map that we are going to use in order to construct these new codes (we have $n = q^{2\ell-1}+1$):

$$\mathrm{ev}_{\mathrm{Tr}^{\mathrm{s}}_{2\mathrm{r}}} : \mathbb{F}_{q^{2\ell}}[x_0,x_1]/I(X_{\mathrm{Tr}^{\mathrm{s}}_{2\mathrm{r}}}) \to \mathbb{F}_{q^{2\ell}}^n,\ \ f \mapsto (f(P_1),\ldots,f(P_n))_{P_i \in X_{\mathrm{Tr}^{\mathrm{s}}_{2\mathrm{r}}}}.$$

Definition B.6.3. Let $\mathcal{A} = \{a_0 = 0 < a_1 < \cdots < a_z\}$. We are going to consider a set $\Delta = \bigcup_{i=0}^{t-1} \mathfrak{I}_{a_i} \cup \{a_t\}$ as before. For such a set Δ, we consider the code $\mathcal{D}(\mathrm{Tr}^{\mathrm{s}}_{2\mathrm{r}}, \Delta)$ defined as the linear code generated by $\{\mathrm{ev}_{\mathrm{Tr}^{\mathrm{s}}_{2\mathrm{r}}}(x_0x_1^{\alpha}) \mid \alpha \in \Delta \setminus \{a_t\}\} \cup \{\mathrm{ev}_{\mathrm{Tr}^{\mathrm{s}}_{2\mathrm{r}}}(x_1^{a_t})\}$.

In what follows we are going to need to use the codes $\mathrm{RS}(\mathrm{Tr}^{\mathrm{s}}_{2\mathrm{r}}, \Delta) := \mathrm{RS}(Y_{\mathrm{Tr}^{\mathrm{s}}_{2\mathrm{r}}}, \Delta)$ that appear in [18], which are the puncturing of the codes $\mathcal{D}(\mathrm{Tr}^{\mathrm{s}}_{2\mathrm{r}}, \Delta)$ at the coordinate associated to the point $[0:1]$. When Δ is a union of consecutive cyclotomic sets, we have that $(\mathrm{RS}(\mathrm{Tr}^{\mathrm{s}}_{2\mathrm{r}}, \Delta)_{q^2})^{\perp} = (\mathrm{RS}(\mathrm{Tr}^{\mathrm{s}}_{2\mathrm{r}}, \Delta)^{\perp})_{q^2}$. We are going to be interested in the code $(\mathcal{D}(\mathrm{Tr}^{\mathrm{s}}_{2\mathrm{r}}, \Delta)^{\perp})_{q^2}$, for which we have the following result.

Theorem B.6.4. *Let* $a_0 = 0 < a_1 < a_2 < \cdots < a_{t-1} < a_t < q^{2\ell}-1$ *be a sequence of consecutive elements of* $\mathcal{A}$. *Let* $\Delta = \bigcup_{i=0}^{t-1} \mathfrak{I}_{a_i} \cup \{a_t\}$ *and let* $\Delta'' = \Delta \cup \mathfrak{I}_{a_t}$. *Assuming that* $(\mathcal{D}(\mathrm{Tr}^{\mathrm{s}}_{2\mathrm{r}}, \Delta)^{\perp})_{q^2}$ *is not degenerate, we have the following inequalities:*

$$\dim\left(\mathcal{D}(\mathrm{Tr}^{\mathrm{s}}_{2\mathrm{r}}, \Delta)^{\perp}\right)_{q^2} = \dim(\mathrm{RS}(\mathrm{Tr}^{\mathrm{s}}_{2\mathrm{r}}, \Delta'')^{\perp})_{q^2} + 1 \geq n - \sum_{i=0}^{t} n_{a_i},$$

$$\mathrm{wt}((\mathcal{D}(\mathrm{Tr}^{\mathrm{s}}_{2\mathrm{r}}, \Delta)^{\perp})_{q^2}) \geq a_t + 2.$$

Proof. By the definitions, it is clear that $\mathcal{D}(\mathrm{Tr}^{\mathrm{s}}_{2\mathrm{r}}, \Delta) = (\mathrm{RS}(\mathrm{Tr}^{\mathrm{s}}_{2\mathrm{r}}, \Delta'), 0) + \langle \mathrm{ev}_{\mathrm{Tr}^{\mathrm{s}}_{2\mathrm{r}}}(x_1^{a_t})\rangle$, where $\Delta' = \Delta \setminus \{a_t\}$. Hence, $\dim \mathcal{D}(\mathrm{Tr}^{\mathrm{s}}_{2\mathrm{r}}, \Delta) = \dim \mathrm{RS}(\mathrm{Tr}^{\mathrm{s}}_{2\mathrm{r}}, \Delta') + 1 = \dim \mathrm{RS}(\mathrm{Tr}^{\mathrm{s}}_{2\mathrm{r}}, \Delta)$, because if we have $\dim \mathrm{RS}(\mathrm{Tr}^{\mathrm{s}}_{2\mathrm{r}}, \Delta') = \dim \mathrm{RS}(\mathrm{Tr}^{\mathrm{s}}_{2\mathrm{r}}, \Delta)$, this means that $\mathrm{ev}_{\mathrm{Tr}^{\mathrm{s}}_{2\mathrm{r}}}(x_0x_1^{a_t})$ is in $(\mathrm{RS}(\mathrm{Tr}^{\mathrm{s}}_{2\mathrm{r}}, \Delta'), 0)$, which implies that $\mathrm{ev}_{\mathrm{Tr}^{\mathrm{s}}_{2\mathrm{r}}}(x_0x_1^{a_t} - x_1^{a_t})$ is in $\mathcal{D}(\mathrm{Tr}^{\mathrm{s}}_{2\mathrm{r}}, \Delta)$, but this is a vector of weight 1, which is a contradiction because $(\mathcal{D}(\mathrm{Tr}^{\mathrm{s}}_{2\mathrm{r}}, \Delta)^{\perp})_{q^2}$ (and $\mathcal{D}(\mathrm{Tr}^{\mathrm{s}}_{2\mathrm{r}}, \Delta)^{\perp}$) is not degenerate. Therefore, we have that $\dim \mathcal{D}(\mathrm{Tr}^{\mathrm{s}}_{2\mathrm{r}}, \Delta)^{\perp} = \dim \mathrm{RS}(\mathrm{Tr}^{\mathrm{s}}_{2\mathrm{r}}, \Delta)^{\perp} + 1$.

Arguing as in the proof of Theorem B.5.5, we have $\mathcal{D}(\mathrm{Tr}^{\mathrm{s}}_{2\mathrm{r}}, \Delta)^{\perp} = (\mathrm{RS}(\mathrm{Tr}^{\mathrm{s}}_{2\mathrm{r}}, \Delta)^{\perp}, 0) + \langle w\rangle$, where w is a vector with a nonzero last entry, and we also obtain $(\mathcal{D}(\mathrm{Tr}^{\mathrm{s}}_{2\mathrm{r}}, \Delta)^{\perp})_{q^2} = ((\mathrm{RS}(\mathrm{Tr}^{\mathrm{s}}_{2\mathrm{r}}, \Delta)^{\perp})_{q^2}, 0) + \langle w'\rangle$ for some vector w' with nonzero last coordinate. Moreover, a basis for $((\mathrm{RS}(\mathrm{Tr}^{\mathrm{s}}_{2\mathrm{r}}, \Delta)^{\perp})_{q^2}, 0)$ would give us $\dim(\mathrm{RS}(\mathrm{Tr}^{\mathrm{s}}_{2\mathrm{r}}, \Delta)^{\perp})_{q^2}$ linearly independent vectors with last coordinate equal to 0, which means that $\dim\left(\mathcal{D}(\mathrm{Tr}^{\mathrm{s}}_{2\mathrm{r}}, \Delta)^{\perp}\right)_{q^2} = \dim(\mathrm{RS}(\mathrm{Tr}^{\mathrm{s}}_{2\mathrm{r}}, \Delta)^{\perp})_{q^2} + 1$.

We obtain $\dim\left(\mathcal{D}(\mathrm{Tr}_{2\mathrm{r}}^{\mathrm{s}},\Delta)^{\perp}\right)_{q^2} = \dim(\mathrm{RS}(\mathrm{Tr}_{2\mathrm{r}}^{\mathrm{s}},\Delta'')^{\perp})_{q^2}+1$ because $(\mathrm{RS}(\mathrm{Tr}_{2\mathrm{r}}^{\mathrm{s}},\Delta)^{\perp})_{q^2} = (\mathrm{RS}(\mathrm{Tr}_{2\mathrm{r}}^{\mathrm{s}},\Delta'')^{\perp})_{q^2}$, which is what we are going to see next. When evaluating in all the points of $\mathbb{F}_{q^{2\ell}}$, we have $(\mathrm{RS}(q^{2\ell},\Delta)^{\perp})_{q^2} = (\mathrm{RS}(q^{2\ell},\Delta'')^{\perp})_{q^2}$. The code $\mathrm{RS}(\mathrm{Tr}_{2\mathrm{r}}^{\mathrm{s}},\Delta)$ (resp. $\mathrm{RS}(\mathrm{Tr}_{2\mathrm{r}}^{\mathrm{s}},\Delta'')$) corresponds to a puncturing of $\mathrm{RS}(q^{2\ell},\Delta)$ (resp. $\mathrm{RS}(q^{2\ell},\Delta'')$) because we only evaluate in the zeroes of $\mathrm{Tr}_{2\mathrm{r}}^{\mathrm{s}}(x)$. The dual of a punctured code is equal to the shortening of the dual code at the same positions [32, Prop. 2.1.17]. Given a code C, if we denote by S the positions where we are puncturing (resp. shortening), by C_S the punctured code and by C^S the shortened code, we obtain

$$((C_S)^{\perp})_{q^2} = ((C^{\perp})^S)_{q^2} = ((C^{\perp})_{q^2})^S,$$

because shortening a code commutes with considering its subfield subcode. Let S be the positions where we puncture in order to obtain $\mathrm{RS}(\mathrm{Tr}_{2\mathrm{r}}^{\mathrm{s}},\Delta)$ from $\mathrm{RS}(q^{2\ell},\Delta)$. Using the previous expression and the fact that $(\mathrm{RS}(q^{2\ell},\Delta)^{\perp})_{q^2} = (\mathrm{RS}(q^{2\ell},\Delta'')^{\perp})_{q^2}$ we get

$$\begin{aligned}(\mathrm{RS}(\mathrm{Tr}_{2\mathrm{r}}^{\mathrm{s}},\Delta)^{\perp})_{q^2} &= ((\mathrm{RS}(q^{2\ell},\Delta)_S)^{\perp})_{q^2} = ((\mathrm{RS}(q^{2\ell},\Delta)^{\perp})_{q^2})^S = ((\mathrm{RS}(q^{2\ell},\Delta'')^{\perp})_{q^2})^S \\ &= ((\mathrm{RS}(q^{2\ell},\Delta'')_S)^{\perp})_{q^2} = (\mathrm{RS}(\mathrm{Tr}_{2\mathrm{r}}^{\mathrm{s}},\Delta'')^{\perp})_{q^2}.\end{aligned}$$

The bound for the dimension given in the statement is obtained by using [18, Thm. 13].

On the other hand, for the minimum distance, we have the BCH-type bound for $\mathcal{D}(\mathrm{Tr}_{2\mathrm{r}}^{\mathrm{s}},\Delta)^{\perp}$, which gives $\mathrm{wt}(\mathcal{D}(\mathrm{Tr}_{2\mathrm{r}}^{\mathrm{s}},\Delta)^{\perp}) \geq a_t+2$, and it is inherited by $(\mathcal{D}(\mathrm{Tr}_{2\mathrm{r}}^{\mathrm{s}},\Delta)^{\perp})_{q^2}$. □

The previous result shows that, if $a_{t+1}+1 = a_t+2$, then the code $(\mathcal{D}(\mathrm{Tr}_{2\mathrm{r}}^{\mathrm{s}},\Delta)^{\perp})_{q^2}$ has 1 more length and dimension than the code $(\mathrm{RS}(\mathrm{Tr}_{2\mathrm{r}}^{\mathrm{s}},\Delta'')^{\perp})_{q^2}$. In the next example we obtain some codes $(\mathcal{D}(\mathrm{Tr}_{2\mathrm{r}}^{\mathrm{s}},\Delta)^{\perp})_{q^2}$ with record parameters according to [21].

Example B.6.5. We consider the field extension $\mathbb{F}_{2^8} \supset \mathbb{F}_{2^2}$, i.e., we have $q=2$ and $\ell=4$. Therefore, we will get codes with length $N=129$. Let $\Delta = \mathfrak{I}_0 \cup \mathfrak{I}_1 \cup \cdots \mathfrak{I}_{a_{t-1}} \cup \{a_t\}$. Hence, we have $\mathrm{wt}\left((\mathcal{D}(\mathrm{Tr}_{2\mathrm{r}}^{\mathrm{s}},\Delta)^{\perp})_{q^2}\right) \geq a_t+2$. The dimension of these codes can be easily computed using Magma [5]. In this case, we obtain a lot of codes whose parameters achieve the best known values in [21], and in many cases we are obtaining codes with higher length and dimension, but same minimum distance as in the affine case. Moreover, we obtain the parameters $[129,90,15]_4$, $[129,86,16]_4$ and $[129,41,44]_4$, for a_t equal to 13, 14 and 42, respectively. In [21], a construction of a code with parameters $[129,86,16]_4$ is currently missing, and we are able to obtain one. The codes with parameters $[129,90,15]_4$ and $[129,41,44]_4$ exceed the best known values in [21]. Furthermore, by shortening and puncturing these codes we are able to obtain more codes with record parameters or missing constructions in [21]. For instance, from the code with parameters $[129,41,44]_4$, we obtain the parameters $[129-i-j, 41-i, 44-j]_4$, for $0 \leq i \leq 4$, $0 \leq j \leq 3$, which are either records or the construction of a code with those parameters is missing in [21].

The next result shows that we can construct quantum codes over $\mathbb{F}_q$ using Theorem B.6.4 together with the Hermitian construction B.5.14.

Theorem B.6.6. *Let $\mathcal{A} = \{a_0 = 0 < a_1 < a_2 < \cdots < a_z\}$ be the set of minimal representatives of the cyclotomic sets $\mathfrak{I}_{a_i}$, $0 \leq i \leq z$, of $\{0,1,\ldots,q^{2l}-1\}$ with respect to q^2. Let $t \leq z$ be an index such that*

$$a_t \leq q^{\ell} - \left\lfloor \frac{(q-1)}{2} \right\rfloor q^{\ell-1} - \cdots - \left\lfloor \frac{(q-1)}{2} \right\rfloor q - 1.$$

Then, for $\Delta = \bigcup_{i=0}^{t-1} \mathfrak{I}_{a_i} \cup \{a_t\}$ *as before, assuming that* $(\mathcal{D}(\mathrm{Tr}_{2\mathrm{r}}^{\mathrm{s}}, \Delta)^{\perp})_{q^2}$ *is not degenerate, we have that:*

$$\dim\left(((\mathcal{D}(\mathrm{Tr}_{2\mathrm{r}}^{\mathrm{s}}, \Delta)^{\perp})_{q^2})^{\perp_h} \cap (\mathcal{D}(\mathrm{Tr}_{2\mathrm{r}}^{\mathrm{s}}, \Delta)^{\perp})_{q^2}\right) \geq \dim\left((\mathcal{D}(\mathrm{Tr}_{2\mathrm{r}}^{\mathrm{s}}, \Delta)^{\perp})_{q^2})^{\perp_h} - 1.$$

As a consequence, we can construct an EAQECC with parameters

$$[[n, \geq n - 2\sum_{i=0}^{t} n_{a_i} + c, \geq a_t + 2; c]]_q,$$

where $n = q^{2\ell-1} + 1$ *and* $c \leq 1$.

Proof. Similarly to the proof of Theorem B.5.15, we are going to consider the code $C = ((\mathcal{D}(\mathrm{Tr}_{2\mathrm{r}}^{\mathrm{s}}, \Delta)^{\perp})_{q^2})^{\perp_h}$ for the Hermitian construction B.5.14. By Theorem B.6.4 we obtain the bound for the minimum distance, and we also obtain that $\dim\left((\mathcal{D}(\mathrm{Tr}_{2\mathrm{r}}^{\mathrm{s}}, \Delta)^{\perp})_{q^2})^{\perp_h}\right) \leq \sum_{i=0}^{t} n_{a_i}$, which explains the dimension of the quantum code. The only thing left to prove is the claim about the intersection of $(\mathcal{D}(\mathrm{Tr}_{2\mathrm{r}}^{\mathrm{s}}, \Delta)^{\perp})_{q^2}$ with its hermitian dual.

Under our assumptions, in [18, Thm. 15] it is proved that we have $\mathrm{RS}(\mathrm{Tr}_{2\mathrm{r}}^{\mathrm{s}}, \Delta'')_{q^2} \subset (\mathrm{RS}(\mathrm{Tr}_{2\mathrm{r}}^{\mathrm{s}}, \Delta'')_{q^2})^{\perp_h}$ for $\Delta'' = \bigcup_{i=0}^{t} \mathfrak{I}_{a_i}$. The reasoning from the proof of Theorem B.5.15 finishes the proof. □

Example B.6.7. We continue with Example B.6.5. For $a_t = 10$, we have $a_t + 2 = 12$, and, computing the dimension with Magma [5], we obtain a quantum code with parameters $[[129, 67, 12; 1]]_2$ using Theorem B.6.6. In the affine case from [18], the parameters $[[128, 65, 12; 0]]_2$ are obtained. Therefore, we have increased the length by 1 and the dimension by 2, at the expense of increasing the parameter c by 1. Moreover, the codes $[[129, 73, 11; 1]]_2$, $[[129, 67, 12; 1]]_2$ and $[[129, 59, 13; 1]]_2$ that we can obtain in this way (by changing a_t) cannot be deduced using the propagation rules from [29] with the codes in the table of QECCs from [21].

In [18], the authors consider what they call *complementary codes*, which are obtained in an analogous way, but evaluating in precisely all the points in $\mathbb{F}_{q^{2\ell}}$ besides the zeroes of $\mathrm{Tr}_{2\mathrm{r}}^{\mathrm{s}}(x)$. For the projective case, it is easy to see that including the point at infinity in this set corresponds to considering the zero set of

$$\frac{x_0 x_1^{q^{2\ell}} - x_0^{q^{2\ell}} x_1}{\mathrm{Tr}_{2\mathrm{r}}^{\mathrm{s}}(x_1)^h}.$$

All the results we have given in this section apply to these types of codes as well, but with length $q^{2\ell} - q^{2\ell-1} + 1$ (instead of $q^{2\ell-1} + 1$).

Declarations

Conflict of interest

The authors declare that they have no conflict of interest.

Bibliography

[1] S. E. Anderson, E. Camps-Moreno, H. H. López, G. L. Matthews, D. Ruano, and I. Soprunov. Relative hulls and quantum codes. *IEEE Trans. Inform. Theory*, 70(5):3190–3201, 2024.

[2] J. Bierbrauer. The theory of cyclic codes and a generalization to additive codes. *Des. Codes Cryptogr.*, 25(2):189–206, 2002.

[3] J. Bierbrauer and Y. Edel. New code parameters from Reed-Solomon subfield codes. *IEEE Trans. Inform. Theory*, 43(3):953–968, 1997.

[4] J. Bierbrauer and Y. Edel. Quantum twisted codes. *J. Combin. Des.*, 8(3):174–188, 2000.

[5] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[6] T. Brun, I. Devetak, and M.-H. Hsieh. Correcting quantum errors with entanglement. *Science*, 314(5798):436–439, 2006.

[7] A. R. Calderbank and P. W. Shor. Good quantum error-correcting codes exist. *Phys. Rev. A*, 54:1098–1105, Aug 1996.

[8] S. D. Cohen. Primitive elements and polynomials with arbitrary trace. *Discrete Math.*, 83(1):1–7, 1990.

[9] D. A. Cox, J. Little, and D. O'Shea. *Ideals, varieties, and algorithms.* Undergraduate Texts in Mathematics. Springer, Cham, fourth edition, 2015. An introduction to computational algebraic geometry and commutative algebra.

[10] P. Delsarte. On subfield subcodes of modified Reed-Solomon codes. *IEEE Trans. Inform. Theory*, IT-21(5):575–576, 1975.

[11] I. M. Duursma, C. Rentería, and H. Tapia-Recillas. Reed-Muller codes on complete intersections. *Appl. Algebra Engrg. Comm. Comput.*, 11(6):455–462, 2001.

[12] D. Eisenbud. *Commutative algebra*, volume 150 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1995. With a view toward algebraic geometry.

[13] C. Galindo, O. Geil, F. Hernando, and D. Ruano. New binary and ternary LCD codes. *IEEE Trans. Inform. Theory*, 65(2):1008–1016, 2019.

[14] C. Galindo and F. Hernando. Quantum codes from affine variety codes and their subfield-subcodes. *Des. Codes Cryptogr.*, 76(1):89–100, 2015.

[15] C. Galindo, F. Hernando, R. Matsumoto, and D. Ruano. Entanglement-assisted quantum error-correcting codes over arbitrary finite fields. *Quantum Inf. Process.*, 18(4):Paper No. 116, 18, 2019.

[16] C. Galindo, F. Hernando, R. Matsumoto, and D. Ruano. Asymmetric entanglement-assisted quantum error-correcting codes and bch codes. *IEEE Access*, 8:18571–18579, 2020.

[17] C. Galindo, F. Hernando, and D. Ruano. Stabilizer quantum codes from J-affine variety codes and a new Steane-like enlargement. *Quantum Inf. Process.*, 14(9):3211–3231, 2015.

[18] C. Galindo, F. Hernando, and D. Ruano. Classical and quantum evaluation codes at the trace roots. *IEEE Trans. Inform. Theory*, 65(4):2593–2602, 2019.

[19] C. Galindo, F. Hernando, and D. Ruano. Entanglement-assisted quantum error-correcting codes from RS codes and BCH codes with extension degree 2. *Quantum Inf. Process.*, 20(5):Paper No. 158, 26, 2021.

[20] M. González-Sarabia and C. Rentería. The dual code of some Reed-Muller type codes. *Appl. Algebra Engrg. Comm. Comput.*, 14(5):329–333, 2004.

[21] M. Grassl. Bounds on the minimum distance of linear codes and quantum codes. Online available at `http://www.codetables.de`, 2007. Accessed on 2023-04-04.

[22] M. Hattori, R. J. McEliece, and G. Solomon. Subspace subcodes of Reed-Solomon codes. *IEEE Trans. Inform. Theory*, 44(5):1861–1880, 1998.

[23] F. Hernando, K. Marshall, and M. E. O'Sullivan. The dimension of subcode-subfields of shortened generalized Reed-Solomon codes. *Des. Codes Cryptogr.*, 69(1):131–142, 2013.

[24] F. Hernando, M. E. O'Sullivan, E. Popovici, and S. Srivastava. Subfield-subcodes of generalized toric codes. In *2010 IEEE International Symposium on Information Theory*, pages 1125–1129, 2010.

[25] L. Ioffe and M. Mézard. Asymmetric quantum error-correcting codes. *Phys. Rev. A*, 75:032345, Mar 2007.

[26] M. Kreuzer and L. Robbiano. *Computational commutative algebra. 1*. Springer-Verlag, Berlin, 2000.

[27] G. G. La Guardia. *Quantum error correction—symmetric, asymmetric, synchronizable, and convolutional codes*. Quantum Science and Technology. Springer, Cham, 2020.

[28] H. H. López, I. Soprunov, and R. H. Villarreal. The dual of an evaluation code. *Des. Codes Cryptogr.*, 89(7):1367–1403, 2021.

[29] G. Luo, M. F. Ezerman, M. Grassl, and S. Ling. Constructing quantum error-correcting codes that require a variable amount of entanglement. *Quantum Inf. Process.*, 23(1):Paper No. 4, 28, 2024.

[30] J. Martínez-Bernal, Y. Pitones, and R. H. Villarreal. Minimum distance functions of graded ideals and Reed-Muller-type codes. *J. Pure Appl. Algebra*, 221(2):251–275, 2017.

[31] N. Nakashima and H. Matsui. Decoding of projective reed-muller codes by dividing a projective space into affine spaces. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, E99.A(3):733–741, 2016.

[32] R. Pellikaan, X.-W. Wu, S. Bulygin, and R. Jurrius. *Codes, cryptology and curves with computer algebra*. Cambridge University Press, Cambridge, 2018.

[33] P. K. Sarvepalli, A. Klappenecker, and M. Rötteler. Asymmetric quantum codes: constructions, bounds and performance. *Proc. R. Soc. Lond. Ser. A Math. Phys. Eng. Sci.*, 465(2105):1645–1672, 2009.

Paper C

Subfield subcodes of projective Reed-Muller codes

Philippe Gimenez, Diego Ruano, Rodrigo San-José

Abstract

Explicit bases for the subfield subcodes of projective Reed-Muller codes over the projective plane and their duals are obtained. In particular, we provide a formula for the dimension of these codes. For the general case over the projective space, we generalize the necessary tools to deal with this case as well: we obtain a universal Gröbner basis for the vanishing ideal of the set of standard representatives of the projective space and we show how to reduce any monomial with respect to this Gröbner basis. With respect to the parameters of these codes, by considering subfield subcodes of projective Reed-Muller codes we obtain long linear codes with good parameters over a small finite field.

Keywords: Evaluation codes, linear codes, projective Reed-Muller codes, subfield subcodes, trace.

MSC: 11T71, 94B05, 14G50, 13P25.

DOI: 10.1016/j.ffa.2023.102353

Reference: P. Gimenez, D. Ruano, R. San-José. Subfield subcodes of projective Reed-Muller codes. Finite Fields Appl. 94, 102353 (2024).

Affiliation: Philippe Gimenez, Diego Ruano, Rodrigo San-José: IMUVA-Mathematics Research Institute, Universidad de Valladolid.

C.1 Introduction

The subfield subcode of a linear code $C \subset \mathbb{F}_{q^s}^n$, with $s \geq 1$, is the linear code $C \cap \mathbb{F}_q^n$. This is a standard procedure that may be used to construct long linear codes over a small finite field. For instance, BCH codes can be seen as subfield subcodes of Reed-Solomon codes. In the multivariate case, the subfield subcodes of J-affine variety codes are well known [9] (in particular, the subfield subcodes of Reed-Muller codes) and have been used for several applications [8, 10]. The main problem that arises when working with subfield subcodes is the computation of a basis for the code, which also gives the dimension. In this paper, we compute bases for the subfield subcodes of projective Reed-Muller codes over the projective plane $\mathbb{P}^2$ and for their duals, and we also give tools to study the general case of projective Reed-Muller codes over the projective space $\mathbb{P}^m$.

Projective Reed-Muller codes are evaluation codes obtained by evaluating multivariate homogeneous polynomials in the projective space. Arguing as in [17], when one considers the sum of the rate and the relative minimum distance as a measure of how good the parameters of a code are, we obtain that projective Reed-Muller codes outperform Reed-Muller codes. It is therefore natural to pose the problem of studying the subfield subcodes of projective Reed-Muller codes, in particular, the problem of obtaining bases for the subfield subcode and its dual. As we stated previously, this has been done for different families of evaluation codes over the affine space [9, 14], but for evaluation codes over the projective space this has only been studied for evaluation codes over certain subsets of the projective line [12]. In particular, the subfield subcodes of J-affine variety codes have been used for constructing quantum codes with good parameters [7, 9], and one can expect that the subfield subcodes of projective Reed-Muller will also perform well in that setting.

In Section C.3, we study the subfield subcode of a projective Reed-Muller code over the projective plane $\mathbb{P}^2$ and its dual. Comparing with projective Reed-Muller codes over $\mathbb{P}^m$, with $m > 2$, the case $m = 2$ is usually the most interesting one because it can give rise to long codes with competitive parameters, which is similar to what happens in the affine case with Reed-Muller codes. For the case $m = 2$, we provide explicit bases for both the subfield subcode of a projective Reed-Muller code over the projective plane $\mathbb{P}^2$ and its dual. In order to construct the basis for the dual, we consider Delsarte's Theorem C.2.7, which shows that we can generate the dual of the subfield subcode of a projective Reed-Muller code of degree d by considering the evaluation of the traces of monomials of degree d. Then we can obtain a basis for the code by extracting a maximal linearly independent set of vectors, and we do this by using the vanishing ideal of the projective plane from Lemma C.3.3 and the division by a Gröbner basis of this ideal. For the primary code, we study some polynomials obtained by combining traces of monomials and such that they can be regarded as homogeneous polynomials of degree d. We show that the set formed by their evaluations is linearly independent, and we conclude that this set is a basis for the code by a dimension argument, as we already have a basis of the dual code.

We generalize some of the previous ideas to the general setting of the projective space $\mathbb{P}^m$ in Section C.4. When we consider a larger m, we usually increase the length at the cost of having worse relative parameters, and also the analysis gets more complicated. Nevertheless, we are able to deal with this case as well. We give the vanishing ideal of a certain set of representatives of the points of $\mathbb{P}^m$. We prove that the set of generators that we give is a universal Gröbner basis of the ideal by using Buchberger's criterion [4, §9

Thm. 3, Chapter 2] and showing that all the S-polynomials of the generators reduce to 0, for any monomial order. From this result, we obtain the initial ideal and a basis for the quotient ring. Moreover, we provide a way to obtain the remainder of the division algorithm by this Gröbner basis for any monomial. This can be proved by checking that the remainder that we state is equivalent in the quotient ring to the original monomial, i.e., both have the same evaluation, and then checking that all the monomials in the support of the remainder are part of the basis given for the quotient ring. Particular cases of these ideas have been used previously for the projective line and the projective plane [12, 19], and we showcase them in full generality. With these tools, it is possible to deal with the general case of computing bases for the subfield subcodes of projective Reed-Muller codes over $\mathbb{P}^m$ and their duals, although getting explicit results as in the case $m = 2$ seems out of reach as it gets too technical.

In Section C.5, we provide some examples of subfield subcodes of projective Reed-Muller codes. We compare their parameters with the codes from [13], and we see that some of the codes that we obtain have the best known parameters for the binary and ternary case. When considering longer codes, it is thus expected to also achieve good parameters, although the absence of tables for long codes makes comparisons difficult. One way to see that some of the longer codes also have good parameters is to consider the Gilbert-Varshamov bound [15, Thm. 2.8.1]. We provide a table with several of the codes that we obtain that exceed it.

C.2 Preliminaries

We consider a finite field $\mathbb{F}_q$ of q elements with characteristic p, and its degree s extension $\mathbb{F}_{q^s}$, with $s > 1$. We consider the projective space $\mathbb{P}^m$ over $\mathbb{F}_{q^s}$ and the polynomial ring $S = \mathbb{F}_{q^s}[x_0, \dots, x_m]$. Throughout this work, we will fix representatives for the points of $\mathbb{P}^m$: for each point in $\mathbb{P}^m$, we choose the representative whose first nonzero coordinate is equal to 1, starting from the left. We will denote by P^m the set of representatives that we have chosen (seen as points in the affine space $\mathbb{A}^{m+1}$) and we will call them *standard representatives*. Let $n = |P^m| = \frac{q^{s(m+1)}-1}{q^s-1}$. We consider the following evaluation map:

$$\mathrm{ev}_d : S_d \to \mathbb{F}_{q^s}^n, \;\; f \mapsto (f(Q_1), \dots, f(Q_n))_{Q_i \in P^m} ,$$

where S_d denotes the homogeneous polynomials of degree d. If $m = 1$, the image of this evaluation map is the *projective Reed-Solomon code* of degree d (also called doubly extended Reed-Solomon code), and we will denote it by PRS_d. The parameters of these codes are $[q^s + 1, d + 1, q^s - d + 1]$. If $m > 1$, then the image of the previous evaluation map is the *projective Reed-Muller code* of degree d, which we will denote by $\mathrm{PRM}_d(m)$. This is another well known family of codes [17, 20].

Given a code $C \subset \mathbb{F}_{q^s}^n$, its subfield subcode with respect to the extension $\mathbb{F}_{q^s} \supset \mathbb{F}_q$ is defined as $C^\sigma := C \cap \mathbb{F}_q^n$. Subfield subcodes of projective Reed-Solomon codes, denoted by PRS_d^σ, were studied in [12], and in this paper we are interested in studying the subfield subcodes of projective Reed-Muller codes and their dual codes, denoted by $\mathrm{PRM}_d^\sigma(m)$ and $\mathrm{PRM}_d^{\sigma,\perp}(m)$, respectively. Before studying the projective case, let us show what happens in the affine case.

C.2.1 Subfield subcodes of affine Reed-Muller codes

The subfield subcodes of affine Reed-Muller, and, more generally, J-affine variety codes, are well known [8, 10]. We introduce now some of the basic techniques that are used to study the subfield subcodes of Reed-Muller codes, which we will denote by $\mathrm{RM}_d^q(m)$.

Let $m \geq 1$ be an integer. We consider the ideal I_{q^s} in the ring $R = \mathbb{F}_{q^s}[x_1, \ldots, x_m]$ generated by $x_j^{q^s} - x_j$. It is clear that the finite set of points defined by I_{q^s} is precisely the whole affine space $\mathbb{A}^m$ over $\mathbb{F}_{q^s}$.

Let $n = q^{sm}$. Consider the quotient ring $R_{q^s} = R/I_{q^s}$ and the evaluation map $\mathrm{ev}_{\mathbb{A}^m} : R_{q^s} \to \mathbb{F}_{q^s}^n$ given by

$$\mathrm{ev}_{\mathbb{A}^m}(f) = (f(Q_1), f(Q_2), \ldots, f(Q_n))_{Q_i \in \mathbb{A}^m}.$$

This map is well defined and is clearly an isomorphism of vector spaces because I_{q^s} is the vanishing ideal of $\mathbb{A}^m$. When working over quotient rings, we will use the same letter f to denote the equivalence class and any polynomial representing it.

For $m = 1$, the image by the evaluation map of $R_{\leq d}$, the polynomials of degree less than or equal to d, is the Reed-Solomon code of degree d (sometimes called extended Reed-Solomon code), which we denote by RS_d. For $m \geq 2$, the image by the evaluation map of $R_{\leq d}$ is the Reed-Muller code of degree d.

We introduce now multivariate cyclotomic sets, which are useful for computing the subfield subcodes of Reed-Muller codes. We consider $\mathbb{Z}/\langle q^s - 1\rangle$, where we represent the classes of $\mathbb{Z}/\langle q^s - 1\rangle$ by $\{1, 2, \ldots, q^s - 1\}$, and we define $\mathbb{Z}_{q^s} = \{0\} \cup \mathbb{Z}/\langle q^s - 1\rangle$, where we represent its classes by $\{0, 1, \ldots, q^s - 1\}$. We will call a subset $\mathfrak{I}$ of the Cartesian product $\mathbb{Z}_{q^s}^m := \prod_{i=1}^m \mathbb{Z}_{q^s}$ a *cyclotomic set* with respect to q if $q \cdot c \in \mathfrak{I}$ for any $c \in \mathfrak{I}$. Furthermore, $\mathfrak{I}$ is said to be *minimal* (with respect to q) if it can be expressed as $\mathfrak{I} = \{q^i \cdot c, i = 1, 2, \ldots\}$ for a fixed $c \in \mathfrak{I}$, and in that situation we will write $\mathfrak{I}_c := \mathfrak{I}$ and $n_c = |\mathfrak{I}_c|$.

Now we define the following lexicographic order in the Cartesian product $\mathbb{Z}_{q^s}^m$: $a = (a_1, \ldots, a_m) < (b_1, \ldots, b_m) = b$ if and only if the rightmost entry of $b - a$, viewing this vector in $\mathbb{Z}^m$, is positive. We say that $a \in \mathfrak{I}_c$ is a *minimal representative* of $\mathfrak{I}_c$ if a is the least element in $\mathfrak{I}_c$ according to the order that we have given, and we will say that $b \in \mathfrak{I}_c$ it is a *maximal representative* of $\mathfrak{I}_c$ if it is the biggest element. We will denote by $\mathcal{A}$ the set of minimal representatives of the minimal cyclotomic sets, and by $\mathcal{B}$ the set of maximal representatives of the minimal cyclotomic sets.

We can introduce a notion of degree for the elements in $\mathbb{Z}_{q^s}^m$. Given an integer $d \geq 1$, we define $\Delta_d = \{c = (c_1, c_2, \ldots, c_m) \in \mathbb{Z}_{q^s}^m \mid \sum_{i=1}^m c_i = d\}$, $\Delta_{<d} = \{c = (c_1, c_2, \ldots, c_m) \in \mathbb{Z}_{q^s}^m \mid \sum_{i=1}^m c_i < d\}$ and $\Delta_{\leq d} = \{c = (c_1, c_2, \ldots, c_m) \in \mathbb{Z}_{q^s}^m \mid \sum_{i=1}^m c_i \leq d\}$. We will also denote by $\mathcal{A}_{<d}$ and $\mathcal{A}_{\leq d}$ the elements $a \in \mathcal{A}$ such that $\mathfrak{I}_a \subset \Delta_{<d}$ and $\mathfrak{I}_a \subset \Delta_{\leq d}$, respectively.

Example C.2.1. Consider the extension $\mathbb{F}_4 \supset \mathbb{F}_2$ with $m = 2$. We have $q = 2$ and $q^s = 2^2 = 4$. Therefore, $\mathbb{Z}_4 = \{0\} \cup \mathbb{Z}/\langle 3\rangle$. We have the following minimal cyclotomic sets:

$$\mathfrak{I}_{(0,0)} = \{(0,0)\}, \mathfrak{I}_{(1,0)} = \{(1,0),(2,0)\}, \mathfrak{I}_{(0,1)} = \{(0,1),(0,2)\}, \mathfrak{I}_{(1,1)} = \{(1,1),(2,2)\},$$
$$\mathfrak{I}_{(3,0)} = \{(3,0)\}, \mathfrak{I}_{(0,3)} = \{(0,3)\}, \mathfrak{I}_{(3,3)} = \{(3,3)\}, \mathfrak{I}_{(2,1)} = \{(2,1),(1,2)\},$$
$$\mathfrak{I}_{(1,3)} = \{(1,3),(2,3)\}, \mathfrak{I}_{(3,1)} = \{(3,1),(3,2)\}.$$

The set of minimal representatives is

$$\mathcal{A} = \{(0,0),(1,0),(0,1),(1,1),(3,0),(0,3),(3,3),(2,1),(1,3),(3,1)\},$$

and the set of maximal representatives is:

$$\mathcal{B} = \{(0,0),(2,0),(0,2),(2,2),(3,0),(0,3),(3,3),(1,2),(2,3),(3,2)\}.$$

For each $a \in \mathcal{A}$, we define the following trace map:

$$\mathcal{T}_a : R_{q^s} \to R_{q^s}, \;\; f \mapsto f + f^q + \cdots + f^{q^{(n_a-1)}},$$

where we fix representatives in R_{q^s} as follows: we will choose the representative of f (and $\mathcal{T}_a(f)$) such that the monomials $x_1^{\gamma_1} \cdots x_m^{\gamma_m}$ in its support have their exponents reduced modulo $q^s - 1$, i.e., $0 \leq \gamma_i \leq q^s - 1$, $1 \leq i \leq m$. We will represent elements of R_{q^s} and R in the same way (simply as polynomials). Therefore, sometimes we consider $\mathcal{T}_a(f)$ as a polynomial in R (the representative that we have chosen), which can be seen in other quotient spaces (such as the one we will define for the projective case).

Example C.2.2. Continuing with Example C.2.1, let us consider $a = (2,1)$ and compute $\mathcal{T}_a(x_1^2 x_2)$. We have $n_a = 2$ and, since $x_1^4 = x_1$ in $R_4 = \mathbb{F}_4[x_1, x_2]/\langle x_1^4 - x_1, x_2^4 - x_2\rangle$, then $\mathcal{T}_a(x_1^2 x_2) = x_1^2 x_2 + x_1 x_2^2$ which is the representative of $x_1^2 x_2 + x_1^4 x_2^2$ in R_4 with its exponents reduced modulo $q^s - 1 = 3$.

The following result gives a basis for the subfield subcodes of Reed-Muller codes (and also Reed-Solomon codes) [8, Thm. 11], which we will denote by $\mathrm{RM}_d^\sigma(m)$.

Theorem C.2.3. *Set ξ_a a primitive element of the field $\mathbb{F}_{q^{n_a}}$. A basis for the vector space $\mathrm{RM}_d^\sigma(m)$ is obtained by considering the images under the map $\mathrm{ev}_{\mathbb{A}^m}$ of the set*

$$\bigcup_{a \in \mathcal{A}_{\leq d}} \{\mathcal{T}_a(\xi_a^r x^a) \mid 0 \leq r \leq n_a - 1\}.$$

As a consequence, we have that

$$\dim \mathrm{RM}_d^\sigma(m) = \sum_{a \in \mathcal{A}_{\leq d}} n_a.$$

Remark C.2.4. Theorem C.2.3 implies that, for different cyclotomic sets $\mathfrak{I}_a \neq \mathfrak{I}_b$, the evaluation of the polynomials in the sets $\{\mathcal{T}_a(\xi_a^r x^a) \mid 0 \leq r \leq n_a - 1\}$ and $\{\mathcal{T}_b(\xi_b^r x^b) \mid 0 \leq r \leq n_b - 1\}$ are linearly independent. Moreover, if we have $\mathfrak{I}_a = \mathfrak{I}_b$, then the previous sets generate the same vector space.

C.2.2 Subfield subcodes of projective Reed-Muller codes

Now we introduce the techniques that we will use to compute subfield subcodes of evaluation codes over the projective space. We had previously defined the usual evaluation map ev_d over the projective space, which can be generalized to the evaluation map $\mathrm{ev} : S \to \mathbb{F}_{q^s}^n$ given by

$$\mathrm{ev}(f) = (f(Q_1), f(Q_2), \ldots, f(Q_n))_{Q_i \in P^m}.$$

It is clear that the kernel of the evaluation map is precisely the vanishing ideal of P^m, denoted by $I(P^m)$. If we consider $\mathrm{ev}(S_d)$ (corresponds to projective Reed-Solomon codes or projective Reed-Muller codes), the resulting code will be isomorphic to $S_d/(I(P^m) \cap S_d) \cong (S_d + I(P^m))/I(P^m)$. As we will see throughout this work, the vanishing ideal $I(P^m)$ gives plenty of information about these codes.

Remark C.2.5. Throughout the rest of the paper, given a set of polynomials B, we will refer to the set $\{\mathrm{ev}(f) \mid f \in B\} \subset \mathbb{F}_{q^s}^n$ as the evaluation of the set B.

We will say that $f \in S$ evaluates to $\mathbb{F}_q$ in P^m if $\mathrm{ev}(f) \in \mathbb{F}_q^n$. The following result gives us conditions for a polynomial to evaluate to $\mathbb{F}_q$ in P^m.

Lemma C.2.6. *One has that $f \in k[x_0, \ldots, x_m]$ evaluates to $\mathbb{F}_q$ in P^m if and only if $f(1, x_1, \ldots, x_m)$, $f(0, 1, x_2, \ldots, x_m)$, $f(0, 0, 1, x_3, \ldots, x_m)$,..., and $f(0, 0, \ldots, 0, 1, x_m)$ evaluate to $\mathbb{F}_q$ in $\mathbb{A}^m, \mathbb{A}^{m-1}, \mathbb{A}^{m-2}, \ldots, \mathbb{A}$, respectively, and $f(0, \ldots, 0, 1) \in \mathbb{F}_q$.*

Proof. We can decompose P^m as the following union of affine spaces: $P^m = \bigcup_{i=0}^m A_i$, where $A_i = \{Q = [Q_0 : \cdots : Q_m] \in P^m \mid Q_0 = \cdots = Q_{i-1} = 0, Q_i = 1\}$ if $1 \leq i \leq m$, and $A_0 = \{Q = [Q_0 : \cdots : Q_m] \in P^m \mid Q_0 = 1\}$. Therefore, f evaluates to $\mathbb{F}_q$ in P^m if and only if f evaluates to $\mathbb{F}_q$ in each set A_i, $0 \leq i \leq m$. The evaluation of $\mathbb{F}_q$ at each of the points of the set A_i is the same as the evaluation of $f(0, \ldots, 0, 1, x_{i+1}, \ldots, x_m)$, and the evaluation of this polynomial at the points of A_i is the same as its evaluation in $\mathbb{A}^{m-i}$. □

In order to construct polynomials that evaluate to $\mathbb{F}_q$ in P^m we consider homogenizations of traces of polynomials. Given a polynomial $f \in R = \mathbb{F}_{q^s}[x_1, \ldots, x_m]$, and a degree $d \geq \deg(f)$, we define the homogenization of f up to degree d as

$$f^h = x_0^d f(x_1/x_0, x_2/x_0, \ldots, x_m/x_0) \in S_d = \mathbb{F}_{q^s}[x_0, \ldots, x_m]_d.$$

In what follows, we will always consider some fixed degree d, and, unless stated otherwise, we will assume that we homogenize up to degree d.

Let $d \geq 1$ and let $a \in \mathcal{A}_{\leq d}$. We are interested in homogenizing the polynomials from the basis from Theorem C.2.3. The condition $a \in \mathcal{A}_{\leq d}$ ensures that, with the fixed representatives that we have chosen for $\mathcal{T}_a(f)$ (the exponents of the monomials are reduced modulo $q^s - 1$), we have $\deg(\mathcal{T}_a(f)) \leq d$. Now we can define the following homogenization:

$$\mathcal{T}_a^h : R \to S/I(P^m),\ f \mapsto (\mathcal{T}_a(f))^h, \tag{C.2.1}$$

where we homogenize up to degree d, and we consider that $\mathcal{T}_a(f) \in R$ is the representative that we have chosen in R_{q^s}. Note that the homogenization is not well defined in general for a class in R_{q^s}, which is why we had to fix a representative for $\mathcal{T}_a(f)$.

These homogenized traces have already been used to obtain bases for the subfield subcode of a projective Reed-Solomon code and its dual in [12]. With respect to the dual code of a subfield subcode, we have the following result by Delsarte [5]:

Theorem C.2.7. *Let $C \subset \mathbb{F}_{q^s}^n$ be a linear code.*

$$(C \cap \mathbb{F}_q^n)^\perp = \mathrm{Tr}(C^\perp),$$

where $\mathrm{Tr} : \mathbb{F}_{q^s} \to \mathbb{F}_q$ maps x to $x + x^q + \cdots + x^{q^{s-1}}$ and is applied componentwise to $C^\perp$.

In [12], a basis for the dual of the subfield subcode of a projective Reed-Solomon code was obtained by using the previous result. In the following sections we will generalize these ideas to deal with the case P^m, with $m > 1$.

C.3 Codes over the projective plane

In this section, we focus on the case $X = P^2$, where we can give precise results, although it gets much more technical than the case $m = 1$ from [12]. The goal is to compute bases for $\mathrm{PRM}_d^{\sigma,\perp}(2)$ and $\mathrm{PRM}_d^{\sigma}(2)$ and, in particular, their dimensions. We set $S = \mathbb{F}_{q^s}[x_0, x_1, x_2]$, and consider cyclotomic sets in two coordinates. Here, $\mathcal{A}$ will be the set of minimal representatives of cyclotomic sets in two coordinates, and we will usually use the letters a and c to denote elements (a_1, a_2) and (c_1, c_2) of some cyclotomic sets $\mathfrak{I}_a$ or $\mathfrak{I}_c$. We will also use the univariate cyclotomic sets in this context, and we define $\mathcal{A}^1 := \{a_2 \mid (a_1, a_2) \in \mathcal{A}\}$. Because of the choice of the ordering of the elements in $\mathbb{Z}_{q^s}^2$, $a = (a_1, a_2) \in \mathcal{A}$ verifies that a_2 is a minimal representative of the cyclotomic set $\mathfrak{I}_{a_2}$ in one coordinate. Therefore, $\mathcal{A}^1$ is also the set of minimal representatives of cyclotomic sets in one coordinate. We will use letters a_2 or c_2 (or a letter that clearly corresponds to an integer) to denote the elements of the cyclotomic sets $\mathfrak{I}_{a_2}$ in one coordinate.

The next result summarizes the main consequences of the results of this section. The definitions of $\overline{d}$ and Y can be found in Definition C.3.5 and (C.3.11), respectively.

Theorem C.3.1. *Let $1 \leq d \leq 2(q^s - 1)$. Then the subfield subcode of the projective Reed-Muller code, $\mathrm{PRM}_d^{\sigma}(2)$, is a code with length $n = |P^m| = \frac{q^{m+1}-1}{q-1}$, and dimension*

$$\dim(\mathrm{PRM}_d^{\sigma}(2)) = \sum_{a \in \mathcal{A}_{<d}} n_a + \sum_{a_2 \in Y} n_{a_2} + \epsilon,$$

where, if we consider $b_2 \in \mathcal{A}^1$ with $\mathfrak{I}_{b_2} = \mathfrak{I}_{\overline{d}}$, then $\epsilon = n_{\overline{d}} + 1$ if $\mathfrak{I}_{(q^s-1,\overline{d})} \subset \Delta_{\leq d}$; $\epsilon = 1$ if $\mathfrak{I}_{(q^s-1,\overline{d})} \not\subset \Delta_{\leq d}$ and $\bigcup_{c_2 \in \mathfrak{I}_{b_2}, c_2 > d-(q^s-1)} \mathfrak{I}_{(d-c_2,c_2)} \subset \Delta_{\leq d}$; and $\epsilon = 0$ otherwise. Moreover, the minimum distance is bounded by

$$\mathrm{wt}(\mathrm{PRM}_d^{\sigma}(2)) \geq \mathrm{wt}(\mathrm{PRM}_d(2)) = (q^s - t)q^{s(1-r)},$$

where $d - 1 = r(q^s - 1) + t$, with $0 \leq t < q^s - 1$.

The formula for the dimension in the previous result can be found in Corollary C.3.42. The dimension of $\mathrm{PRM}_d^{\sigma,\perp}(2)$ can be derived from the previous result, but we also provide another formula in Corollary C.3.13. Moreover, in Theorem C.3.39 and Theorem C.3.12 we provide bases for $\mathrm{PRM}_d^{\sigma}(2)$ and $\mathrm{PRM}_d^{\sigma,\perp}(2)$, respectively.

C.3.1 Dual codes of the subfield subcodes of projective Reed-Muller codes

We start by computing a basis for the dual of the subfield subcode of a projective Reed-Muller code since it is slightly easier due to the nature of Delsarte's Theorem, Theorem C.2.7. For this we need the following result from [20] about the dual of a projective Reed-Muller code.

Theorem C.3.2. *Let $m \geq 2$, $1 \leq d \leq m(q^s - 1)$ and $d^\perp = m(q^s - 1) - d$. Then*

$$\begin{aligned} \mathrm{PRM}_d^{\perp}(m) &= \mathrm{PRM}_{d^\perp}(m) && \text{for } d \not\equiv 0 \bmod (q^s - 1), \\ \mathrm{PRM}_d^{\perp}(m) &= \mathrm{PRM}_{d^\perp}(m) + \langle (1, \ldots, 1) \rangle && \text{for } d \equiv 0 \bmod (q^s - 1). \end{aligned}$$

Setting $m = 2$ now, in order to use Delsarte's Theorem C.2.7, it is useful to introduce the following trace map

$$\mathcal{T} : S/I(P^2) \to S/I(P^2), f \mapsto f + f^q + \cdots + f^{q^{s-1}}.$$

With this definition, it is clear that $\mathrm{ev} \circ \mathcal{T} = \mathrm{Tr} \circ \mathrm{ev}$. Hence, the trace code $\mathrm{Tr}(\mathrm{PRM}_d^\perp(m))$ can be seen as the code generated by the evaluation of some traces in this case. In particular, we can consider $\mathcal{T}(S_{d^\perp})$ (if $d \equiv 0 \bmod q^s - 1$, we also consider $\mathcal{T}(\lambda \cdot 1)$, $\lambda \in \mathbb{F}_{q^s}$). The image by the evaluation map of $\mathcal{T}(S_{d^\perp})$ is a system of generators of $\mathrm{Tr}(\mathrm{PRM}_d^\perp(m))$ if $d \not\equiv 0 \bmod q^s - 1$. If we extract a maximal linearly independent set of polynomials from $\mathcal{T}(S_{d^\perp})$, then its image by ev will be a basis for the dual of the subfield subcode.

As we said before, the kernel of the evaluation map is precisely $I(P^2)$, and we have an isomorphism of the primary code with $S/I(P^2)$. The ideal $I(P^2)$ will play a crucial role in understanding linear independence of the polynomials in $\mathcal{T}(S_d)$. Hence, it is helpful to obtain a Gröbner basis for this ideal and a basis for the quotient $S/I(P^2)$. The following result is a consequence of Theorem C.4.1 and Lemma C.4.3, which will be proven in Section C.4.

Lemma C.3.3. *The following polynomials form a universal Gröbner basis of $I(P^2)$:*

$$I(P^2) = \langle x_0^2 - x_0, x_1^{q^s} - x_1, x_2^{q^s} - x_2, (x_0 - 1)(x_1^2 - x_1), (x_0 - 1)(x_1 - 1)(x_2 - 1)\rangle.$$

Moreover, the set of monomials $\{x_1^{a_1}x_2^{a_2}, x_0x_2^{a_2}, x_0x_1 \mid 0 \le a_i \le q^s - 1, 1 \le i \le 2\}$ is a basis for $S/I(P^2)$.

Remark C.3.4. Because of the generator $x_0^2 - x_0$ of the previous ideal, any positive power of x_0 is equivalent to x_0 in the quotient ring. Therefore, any monomial $x_0^{a_0}x_1^{a_1}x_2^{a_2}$ with $a_0 > 0$ is equivalent to $x_0x_1^{a_1}x_2^{a_2}$ in $S/I(P^2)$.

In what follows, we assume $d \not\equiv 0 \bmod q^s - 1$ to avoid making exceptions due to Theorem C.3.2 (we will recover this case later). By Theorem C.2.7 and Theorem C.3.2, we have that $\mathrm{PRM}_d^{\sigma,\perp}(2)$ can be generated by the image by the evaluation map of traces (using the map $\mathcal{T}$) of multiples of the monomials of degree $d^\perp$. We show next that, to obtain a basis for the dual code, it is enough to consider the trace maps $\mathcal{T}_a$ instead of $\mathcal{T}$, which we extend from R_{q^s} to $S/I(P^2)$ in the following way:

$$\mathcal{T}_a : S/I(P^2) \to S/I(P^2), \;\; f \mapsto f + f^q + \cdots + f^{q^{(n_a-1)}},$$

for a certain $a \in \mathcal{A}$.

We consider the trace map from $\mathbb{F}_{q^s}$ to $\mathbb{F}_{q^l}$, $\mathrm{Tr}_{\mathbb{F}_{q^s}/\mathbb{F}_{q^l}}$ (with $l \mid s$): $\mathrm{Tr}_{\mathbb{F}_{q^s}/\mathbb{F}_{q^l}}(x) = x + x^{q^l} + \cdots + x^{q^{l(\frac{s}{l}-1)}}$. By Theorem C.2.7, Theorem C.3.2, and the previous discussion, we have that $\mathrm{Tr}(\mathrm{PRM}_d^\perp(2))$ is generated by the evaluation of $\mathcal{T}(S_{d^\perp})$, which is generated by the set $\{\mathcal{T}(\lambda x^\gamma), \lambda \in \mathbb{F}_{q^s}^*, x^\gamma \in S_{d^\perp}\}$. Let $\lambda \in \mathbb{F}_{q^s}^*$, $\gamma = (\gamma_0, \gamma_1, \gamma_2)$ and $\hat{\gamma} = (\gamma_1, \gamma_2)$. We consider the cyclotomic set $\mathfrak{I}_{\hat{\gamma}}$, and we have that

$$\begin{aligned}
\mathcal{T}(\lambda x^\gamma) \equiv & \lambda x^\gamma + \lambda^q x^{q\gamma} + \cdots + \lambda^{q^{n_{\hat{\gamma}}-1}} x^{q^{n_{\hat{\gamma}}-1}\gamma} \\
& + \lambda^{q^{n_{\hat{\gamma}}}} x^\gamma + \lambda^{q^{n_{\hat{\gamma}}+1}} x^{q\gamma} + \cdots + \lambda^{q^{2n_{\hat{\gamma}}-1}} x^{q^{n_{\hat{\gamma}}-1}\gamma} + \cdots \\
\equiv & \mathrm{Tr}_{\mathbb{F}_{q^s}/\mathbb{F}_{q^{n_{\hat{\gamma}}}}}(\lambda) x^\gamma + (\mathrm{Tr}_{\mathbb{F}_{q^s}/\mathbb{F}_{q^{n_{\hat{\gamma}}}}}(\lambda))^q x^{q\gamma} + \cdots \\
\equiv & \mathcal{T}_{\hat{\gamma}} \left(\mathrm{Tr}_{\mathbb{F}_{q^s}/\mathbb{F}_{q^{n_{\hat{\gamma}}}}}(\lambda) x^\gamma \right) \bmod I(P^2),
\end{aligned} \tag{C.3.1}$$

where, if $\gamma_0 > 0$, we can reduce the exponent of x_0 in each monomial to 1 (see Remark C.3.4), and we are using that $(x_1^{\gamma_1}x_2^{\gamma_2})^{q^{n_{\hat{\gamma}}}} \equiv x_1^{\gamma_1}x_2^{\gamma_2} \bmod S/I(P^2)$. Equation (C.3.1) shows that, for each monomial x^γ, it is enough to consider the traces

$$\{\mathcal{T}_{\hat{\gamma}}(\xi_{\hat{\gamma}}^r x^\gamma) \mid 0 \leq r \leq n_{\hat{\gamma}} - 1\}. \tag{C.3.2}$$

This is because the trace function is surjective, which means that every element of $\mathbb{F}_{q^{n_{\hat{\gamma}}}}$ is obtained as $\mathrm{Tr}_{\mathbb{F}_{q^s}/\mathbb{F}_{q^{n_{\hat{\gamma}}}}}(\lambda)$ for some $\lambda \in \mathbb{F}_{q^s}$. Taking into account the linearity of the trace function, and the fact that $\{1, \xi_{\hat{\gamma}}, \ldots, \xi_{\hat{\gamma}}^{n_{\hat{\gamma}}-1}\}$ constitutes a basis for $\mathbb{F}_{q^{n_{\hat{\gamma}}}}$, we obtain what we stated.

Thus, for computing a basis for $\mathrm{PRM}_d^{\sigma,\perp}(2)$, we just need to consider the union of the sets in (C.3.2), and extract a maximal linearly independent set. In principle, we will not see the dual code as the image by the evaluation map of a set of homogeneous polynomials. This makes Lemma C.3.3 specially valuable in order to argue about linear independence when we consider polynomials of different degree (for homogeneous polynomials, the homogeneous ideal $I(\mathbb{P}^m)$ from [18] can be used to discuss linear independence).

We note that, for $d > 2(q-1)$, $\mathrm{PRM}_d(2)$ is the whole space. Hence, we will always assume that $d \leq 2(q-1)$ in what follows. We introduce now the following sets which play a crucial role in grouping the polynomials in S_d with linearly dependent traces.

Definition C.3.5. Let $1 \leq d \leq 2(q-1)$. For $0 \leq b \leq 2(q-1)$, we define $\overline{b}$ as the representative of $b \bmod (q^s-1)$ between 1 and q^s-1 if $b \neq 0$, and 0 otherwise. For $a = (a_1, a_2) \in \mathcal{A}$, we define

$$M_a(d) = \langle x_0^{b_0} x_1^{b_1} x_2^{b_2} \mid (\overline{b_1}, \overline{b_2}) \in \mathfrak{I}_a, b_0 + b_1 + b_2 = d \rangle \subset S_d.$$

It is clear that the union of these sets contains all the monomials of S_d, which implies that $S_d = \langle \bigcup_{a \in \mathcal{A}} M_a(d) \rangle$. Therefore, we have that $\mathcal{T}(S_d) = \langle \bigcup_{a \in \mathcal{A}} \mathcal{T}(\langle M_a(d) \rangle) \rangle$, where we have used the linearity of $\mathcal{T}$. Thus, in order to obtain a set of polynomials such that its image by the evaluation map is a basis for $\mathrm{PRM}_d^{\sigma,\perp}(2)$, we are going to obtain a basis for $\mathcal{T}(M_a(d))$, for each $a \in \mathcal{A}$, and then consider the union of these bases which, by the previous argument, will generate $\mathcal{T}(S_d)$. We will then extract a basis from this union.

To achieve that, we first introduce the following definition that we use throughout this section.

Definition C.3.6. Let $1 \leq d \leq 2(q^s-1)$. We will say that $M_a(d)$ *contains monomials of the two types* if there are monomials $m_1, m_2 \in M_a(d)$ such that $x_0 \mid m_1$ and $x_0 \nmid m_2$.

Using all the previous notation, we have the following result which translates some conditions on cyclotomic sets into conditions on the sets $M_a(d)$.

Lemma C.3.7. *Let $1 \leq d \leq 2(q^s-1)$. We have the following:*

1. *$M_a(d)$ is not empty if and only if $\mathfrak{I}_a \cap \Delta_{\leq d} \neq \emptyset$.*
2. *x_0 divides some monomial in $M_a(d)$ if and only if $\mathfrak{I}_a \cap \Delta_{<d} \neq \emptyset$.*
3. *x_0 does not divide all the monomials in $M_a(d)$ if and only if $\mathfrak{I}_a \cap (\Delta_d \cup \Delta_{\overline{d}}) \neq \emptyset$.*
4. *$M_a(d)$ contains monomials of the two types if and only if $\mathfrak{I}_a \cap \Delta_{<d} \neq \emptyset$ and $\mathfrak{I}_a \cap (\Delta_d \cup \Delta_{\overline{d}}) \neq \emptyset$.*

5. x_0 does not divide any monomial in $M_a(d) \neq \emptyset$ if and only if $\mathfrak{I}_a \cap \Delta_{\leq d} \subset \Delta_d$.

Proof. The first one is clear from the definitions. We prove (4) first. If $M_a(d)$ contains monomials of the two types, then $M_a(d)$ is not empty, and there is a monomial $x_1^{b_1}x_2^{b_2} \in M_a(d)$. This means that $(\overline{b_1}, \overline{b_2}) \in \mathfrak{I}_a$, and we have $\overline{b_1} + \overline{b_2} \equiv d \bmod (q^s-1)$. Hence, $(\overline{b_1}, \overline{b_2}) \in \mathfrak{I}_a \cap (\Delta_d \cup \Delta_{\overline{d}}) \neq \emptyset$. There is also a monomial $x_0^{c_0}x_1^{c_1}x_2^{c_2} \in M_a(d)$ with $c_0 > 0$, which implies that $\overline{c_1} + \overline{c_2} < d$ and $(\overline{c_1}, \overline{c_2}) \in \mathfrak{I}_a \cap \Delta_{<d}$.

Conversely, if we have $c \in \mathfrak{I}_a$ such that $c_1+c_2 \equiv d \bmod (q^s-1)$, this means that, if $c_1 > 0$, $x_1^{c_1+\lambda(q^s-1)}x_2^{c_2}$ has degree d for some $\lambda \in \{0,1\}$, which means that this monomial would be in $M_a(d)$. If $c_1 = 0$, the same reasoning proves that the monomial $x_2^{c_2+\lambda(q^s-1)}$ would be in $M_a(d)$ for some $\lambda \in \{0,1\}$. Taking into account the condition $\mathfrak{I}_a \cap \Delta_{<d} \neq \emptyset$, there is an element $u \in \mathfrak{I}_a$ such that $x_1^{u_1}x_2^{u_2}$ is of degree less than d. Thus, $x_0^{u_0}x_1^{u_1}x_2^{u_2} \in M_a(d)$, where $u_0 = d - u_1 - u_2$. This proves (4).

By adapting the previous argument, it is easy to prove (2) and (3), and (5) is the negation of (2), taking (1) into account. □

Example C.3.8. We can consider the extension $\mathbb{F}_{16} \supset \mathbb{F}_2$ ($q = 2$, $s = 4$), and the cyclotomic set $\mathfrak{I}_{(0,3)} = \langle (0,3), (0,6), (0,9), (0,12) \rangle$. For $1 \leq d \leq 2$ we have that $M_{(0,3)}(d) = \emptyset$ since $\mathfrak{I}_{(0,3)} \cap \Delta_{\leq 2} = \emptyset$. For $d = 3$, we have $M_{(0,3)}(3) = \langle x_2^3 \rangle$, i.e., x_0 does not divide any monomial in $M_{(0,3)}(3)$ (due to the fact that $\mathfrak{I}_{(0,3)} \cap \Delta_{\leq 3} = \{(0,3)\} \subset \Delta_3$). For $d = 5$ (similarly for $d = 4$), we have that $M_{(0,3)}(5) = \langle x_0^2x_2^3 \rangle$, i.e., x_0 divides all the monomials in $M_{(0,3)}(5)$ (precisely because $\mathfrak{I}_{(0,3)} \cap \Delta_5 = \emptyset$). For $d = 6$ we have $M_{(0,3)}(6) = \langle x_0^3x_2^3, x_2^6 \rangle$, i.e., $M_{(0,3)}(6)$ contains monomials of the two types, since we have $(0,3) \in \mathfrak{I}_{(0,3)} \cap \Delta_{<6}$ and $(0,6) \in \mathfrak{I}_a \cap \Delta_6$. Lastly, if we consider a degree higher than $q^s = 16$, we have to take into account $\overline{d}$. For example, for $d = 18$, we have $M_{(0,3)}(18) = \langle x_0^{15}x_2^3, x_2^{18}, x_0^{12}x_2^6, x_0^9x_2^9, x_0^6x_2^{12} \rangle$. We see that $M_{(0,3)}(18)$ contains monomials of the two types, as we have that $\overline{d} = 3$ and $(0,3) \in \mathfrak{I}_{(0,3)} \cap \Delta_3$, which means that we can consider the monomial $x_2^{18} \equiv x^3 \bmod I(P^2)$, which does not have x_0 in its support.

The following result is a consequence of Lemma C.4.4, which is proved in Section C.4. It will allow us to obtain a basis for $\mathcal{T}(M_a(d))$, for each $a \in \mathcal{A}$, and it can be understood as the remainder after using the multivariate division algorithm of a monomial with respect to the Gröbner basis from Lemma C.3.3.

Lemma C.3.9. *Let a_0, a_1, a_2 be integers, with $a_0, a_1 > 0$. We have that*

$$\begin{aligned} x_0^{a_0}x_1^{a_1}x_2^{a_2} &\equiv x_1^{a_1}x_2^{a_2} + x_0x_2^{a_2} - x_2^{a_2} + x_0x_1 - x_0 - x_1 + 1 \bmod I(P^2) \\ &\equiv x_1^{a_1}x_2^{a_2} + (x_0 - 1)(x_2^{a_2} + x_1 - 1) \bmod I(P^2). \end{aligned}$$

We recall that the kernel of ev is $I(P^2)$. This implies that a set of classes (polynomials) in $S/I(P^2)$ is linearly independent if and only if the evaluation of this set is linearly independent. This is why, in the following, we may argue about linear independence both from the point of view of polynomials in $S/I(P^2)$ and vectors in $\mathbb{F}_{q^s}^n$.

Lemma C.3.10. *Let $a = (a_1, a_2) \in \mathcal{A}$, let ξ_a be a primitive element of $\mathbb{F}_{q^{n_a}}$ and let ξ_{a_2} be a primitive element of $\mathbb{F}_{q^{n_{a_2}}}$. Then the following polynomials constitute a basis in $S/I(P^2)$ for $\mathcal{T}(M_a(d)) = \langle \mathcal{T}(\lambda x_0^{b_0}x_1^{b_1}x_2^{b_2}), \lambda \in \mathbb{F}_{q^s}, x_0^{b_0}x_1^{b_1}x_2^{b_2} \in M_a(d) \rangle$:*

1. *If x_0 divides all the monomials in $M_a(d) \neq \emptyset$:*

$$\{\mathcal{T}_a(\xi_a^r x_0 x_1^{a_1} x_2^{a_2}) \mid 0 \leq r \leq n_a - 1\}.$$

2. *If x_0 does not divide any monomial in $M_a(d) \neq \emptyset$:*

$$\{\mathcal{T}_a(\xi_a^r x_1^{a_1} x_2^{a_2}) \mid 0 \leq r \leq n_a - 1\}.$$

3. *If $M_a(d)$ contains monomials of the two types, and $a_1 = 0$:*

$$\{\mathcal{T}_a(\xi_a^r x_2^{a_2}) \mid 0 \leq r \leq n_a - 1\} \cup \{\mathcal{T}_a(\xi_a^r x_0 x_2^{a_2}) \mid 0 \leq r \leq n_a - 1\}.$$

4. *If $M_a(d)$ contains monomials of the two types, and $a_1 > 0$:*

$$\{\mathcal{T}_a(\xi_a^r x_1^{a_1} x_2^{a_2}) \mid 0 \leq r \leq n_a - 1\} \cup \{(x_0 - 1)(\mathcal{T}_{a_2}(\xi_{a_2}^r x_2^{a_2}) + \mathcal{T}_{a_2}(\xi_{a_2}^r)(x_1 - 1)) \mid 0 \leq r \leq n_{a_2} - 1\}.$$

Proof. The fact that the polynomials of each set $\{\mathcal{T}_a(\xi_a^r x_0^{a_0} x_1^{a_1} x_2^{a_2}), 0 \leq r \leq n_a\}$ are linearly independent can easily be seen since the evaluation of each set $\{\mathcal{T}_a(\xi_a^r x_0^{a_0} x_1^{a_1} x_2^{a_2}), 0 \leq r \leq n_a\}$ in $[\{1\} \times \mathbb{F}_{q^s}^2]$ is the same as the evaluation of $\{\mathcal{T}_a(\xi_a^r x_1^{a_1} x_2^{a_2}), 0 \leq r \leq n_a\}$ in $\mathbb{F}_{q^s}^2$, and we know that the evaluation of this set in $\mathbb{F}_{q^s}^2$ is linearly independent it is part of the basis given in Theorem C.2.3 for the affine case. For each monomial $x_0^{b_0} x_1^{b_1} x_2^{b_2} \in M_a(d)$, because of the discussion that led to (C.3.2), we know that, instead of considering the set $\{\mathcal{T}(\lambda x_0^{b_0} x_1^{b_1} x_2^{b_2}), \lambda \in \mathbb{F}_{q^s}\}$, it is enough to consider the set $\{\mathcal{T}_a(\xi_a^r x_0^{b_0} x_1^{b_1} x_2^{b_2}), 0 \leq r \leq n_a\}$.

Therefore, if we consider $x_0^{b_0} x_1^{b_1} x_2^{b_2}, x_0^{c_0} x_1^{c_1} x_2^{c_2} \in M_a(d)$, with $b_0, c_0 > 0$, we know that it is sufficient to consider the traces $\{\mathcal{T}_a(\xi_a^r x_0^{b_0} x_1^{b_1} x_2^{b_2}), 0 \leq r \leq n_a - 1\}$ and $\{\mathcal{T}_b(\xi_b^r x_0^{c_0} x_1^{c_1} x_2^{c_2}), 0 \leq r \leq n_a - 1\}$ for each monomial, respectively. However, the evaluations of these sets of traces generate the same space in $[\{1\} \times \mathbb{F}_{q^s}^2]$ due to Theorem C.2.3 and Remark C.2.4, and in the rest of the points both sets of polynomials evaluate to 0. For the case with $b_0 = c_0 = 0$, we just need to observe that the evaluation of any polynomial $f(x_1, x_2)$ in P^2 is fixed by its evaluation in $[\{1\} \times \mathbb{F}_{q^s}^2]$. By the same argument as before, the evaluations of the two sets of polynomials we are considering in $[\{1\} \times \mathbb{F}_{q^s}^2]$ generate the same space, and by the previous observation this implies that their evaluations over P^2 generate the same vector space.

Hence, if we consider the traces of the monomials in $M_a(d)$, it is enough to consider the traces of a monomial divisible by x_0 (if any) and the traces of a monomial not divisible by x_0 (if any). In fact, we can assume that we are considering the monomials $x_0 x_1^{a_1} x_2^{a_2}$ and $x_1^{a_1} x_2^{a_2}$, as any other choice for a monomial that is divisible by x_0 and a monomial that is not divisible by x_0, respectively, would span the same space when considering the space generated by the traces. In the case where $M_a(d)$ only has monomials of one of those types, we know that those traces are linearly independent and we obtain the cases (1) and (2). Another easy case is when $a_1 = 0$, in which, if $M_a(d)$ contains monomials of the two types, we just obtain the polynomials

$$\{\mathcal{T}_a(\xi_a^r x_2^{a_2}) \mid 0 \leq r \leq n_a - 1\} \cup \{\mathcal{T}_a(\xi_a^r x_0 x_2^{a_2}) \mid 0 \leq r \leq n_a - 1\}.$$

We have seen that both of these sets are linearly independent, and when we consider the union we still keep the linear independence since the monomials of each of these traces are

part of the basis in Lemma C.3.3 and both sets have disjoint support for their polynomials. This corresponds to the case (3).

The case where $a_1 > 0$ and $M_a(d)$ contains monomials of the two types is more involved. By the previous discussion, it is enough to consider the sets of polynomials $\{\mathcal{T}_a(\xi_a^r x_0 x_1^{a_1} x_2^{a_2}), 0 \leq r \leq n_a - 1\}$ and $\{\mathcal{T}_a(\xi_a^r x_1^{a_1} x_2^{a_2}), 0 \leq r \leq n_a - 1\}$ for generating $\mathcal{T}(M_a(d))$, and we are interested in knowing how many linearly independent polynomials in $S/I(P^2)$ there are in the union of those sets. In order to construct a basis for the space generated by all these polynomials, we start with the polynomials in $\{\mathcal{T}_a(\xi_a^r x_1^{a_1} x_2^{a_2}), 0 \leq r \leq n_a\}$, and we will check which polynomials from the other set can be included without losing linear independence. First, by Lemma C.3.9, we have that

$$x_0^{q^l a_0} x_1^{q^l a_1} x_2^{q^l a_2} \equiv x_1^{q^l a_1} x_2^{q^l a_2} + (x_0 - 1)(x_2^{q^l a_2} + x_1 - 1) \bmod I(P^2).$$

Thus, for $a = (a_1, a_2)$ with $a_1 > 0$, we consider $\mathfrak{I}_a$ and ξ_a a primitive element of $\mathbb{F}_{q^{n_a}}$, and we obtain

$$\begin{aligned}\mathcal{T}_a(\xi_a^r x_0^{a_0} x_1^{a_1} x_2^{a_2}) &\equiv \mathcal{T}_a(\xi_a^r x_1^{a_1} x_2^{a_2}) + (x_0 - 1) \sum_{l=0}^{n_a - 1} \xi_a^{q^l r} (x_2^{q^l a_2} + x_1 - 1) \bmod I(P^2) \\ &\equiv \mathcal{T}_a(\xi_a^r x_1^{a_1} x_2^{a_2}) + (x_0 - 1)(\mathcal{T}_a(\xi_a^r x_2^{a_2}) + \mathcal{T}_a(\xi_a^r)(x_1 - 1)) \bmod I(P^2).\end{aligned} \tag{C.3.3}$$

By (C.3.3), we obtain that we have to see which polynomials of the type

$$(x_0 - 1)(\mathcal{T}_a(\xi_a^r x_2^{a_2}) + \mathcal{T}_a(\xi_a^r)(x_1 - 1)) = (x_0 - 1)\mathcal{T}_a(\xi_a^r x_2^{a_2}) + (x_0 - 1)(x_1 - 1)\mathcal{T}_a(\xi_a^r) \tag{C.3.4}$$

can be included in the basis that we are constructing without losing linear independence. We note that the exponents of x_2 in these polynomials are precisely the elements of $\mathfrak{I}_{a_2}$. In fact, these polynomials are closely related to the corresponding traces of $\mathfrak{I}_{a_2}$. Arguing as we did to get (C.3.1), we obtain that

$$\mathcal{T}_a(\xi_a^r x_2^{a_2}) = \mathcal{T}_{a_2}\left(\mathrm{Tr}_{\mathbb{F}_{q^{n_a}}/\mathbb{F}_{q^{n_{a_2}}}}(\xi_a^r) x_2^{a_2}\right). \tag{C.3.5}$$

By the argument we used to get (C.3.2), we see that the set $\{\mathcal{T}_{a_2}(\xi_{a_2}^r x_2^{a_2}) \mid 0 \leq r \leq n_{a_2} - 1\}$, where ξ_{a_2} is a primitive element of $\mathbb{F}_{q^{n_{a_2}}}$, generates the same vector space as $\{\mathcal{T}_a(\xi_a^r x_2^{a_2}) \mid 0 \leq r \leq n_a - 1\}$. This implies that the set of polynomials

$$\{(x_0 - 1)(\mathcal{T}_a(\xi_a^r x_2^{a_2}) + \mathcal{T}_a(\xi_a^r)(x_1 - 1)) \mid 0 \leq r \leq n_a\}$$

generates the same space as the set

$$\{(x_0 - 1)(\mathcal{T}_{a_2}(\xi_{a_2}^r x_2^{a_2}) + \mathcal{T}_{a_2}(\xi_{a_2}^r)(x_1 - 1)) \mid 0 \leq r \leq n_{a_2}\}.$$

This is because the same linear combination that expresses $\mathcal{T}_a(\xi_a^r x_2^{a_2})$ in terms of the traces $\mathcal{T}_{a_2}(\xi_{a_2}^r x_2^{a_2})$ also gives $\mathcal{T}_a(\xi_a^r)$ in terms of the traces $\mathcal{T}_{a_2}(\xi_{a_2}^r)$ (we just evaluate $x_2 = 1$), and vice versa. Thus, when considering the polynomials from (C.3.4) that we have to include, is is enough to consider

$$\{(x_0 - 1)(\mathcal{T}_{a_2}(\xi_{a_2}^r x_2^{a_2}) + \mathcal{T}_{a_2}(\xi_{a_2}^r)(x_1 - 1)) \mid 0 \leq r \leq n_{a_2} - 1\}, \tag{C.3.6}$$

which are linearly independent since they coincide with the univariate affine case from Theorem C.2.3 when we evaluate in the points of $[\{0\} \times \{1\} \times \mathbb{F}_{q^s}]$. Finally, when we consider the union of those polynomials with the set $\{\mathcal{T}_a(\xi_a^r x_1^{a_1} x_2^{a_2}), 0 \leq r \leq n_a\}$, we see that they are linearly independent because the polynomials from (C.3.6) evaluate to the zero vector in $[\{1\} \times \mathbb{F}_{q^s}^2]$, while the polynomials from the set $\{\mathcal{T}_a(\xi_a^r x_1^{a_1} x_2^{a_2}), 0 \leq r \leq n_a\}$ give linearly independent vectors when evaluating in $[\{1\} \times \mathbb{F}_{q^s}^2]$. □

By Lemma C.3.10, if x_0 divides all the monomials from $M_a(d)$, or does not divide any of the monomials in $M_a(d)$, we only have to consider n_a polynomials for each $a \in \mathcal{A}$ to construct a basis for $\mathcal{T}(M_a(d))$. However, if $M_a(d)$ contains monomials of the two types we have to consider $n_a + n_{a_2}$ polynomials (note that for $a_1 = 0$ we have $a = (0, a_2)$ and $2n_a = 2n_{a_2} = n_a + n_{a_2}$).

Remark C.3.11. We note that if $a_1 = 0$ and $M_a(d)$ contains monomials of the two types, this means that $x_2^d \in M_a(d)$, which implies that $\overline{d} \in \mathfrak{I}_{a_2}$. Therefore, the case (3) in Lemma C.3.10 applies only to $(0, \overline{d}) \in \mathcal{A}$, and only when $M_{(0,\overline{d})}$ contains monomials of the two types.

Let $d^\perp = 2(q-1) - d$. We introduce the following notation to state the main result of this section. For each $a \in \mathcal{A}$ such that $M_a(d^\perp) \neq \emptyset$, let ξ_a be a primitive element in $\mathbb{F}_{q^{n_a}}$, and consider the following set:

(a) If x_0 divides all the monomials from $M_a(d^\perp)$, we set

$$T_a = \{\mathcal{T}_a(\xi_a^r x_0 x_1^{a_1} x_2^{a_2}) \mid 0 \leq r \leq n_a - 1\}.$$

(b) We set

$$T_a = \{\mathcal{T}_a(\xi_a^r x_1^{a_1} x_2^{a_2}) \mid 0 \leq r \leq n_a - 1\}$$

otherwise.

The reasoning behind T_a is that for any $a \in \mathcal{A}$ such that $M_a(d^\perp) \neq \emptyset$, from Lemma C.3.10 we obtain that T_a is a set of linearly independent polynomials in $\mathcal{T}(M_a(d^\perp))$. We define $U = \{a \in \mathcal{A} \mid M_a(d^\perp) \neq \emptyset\}$, and we consider the union of the previous sets:

$$D_1 = \bigcup_{a \in U} T_a.$$

This is one of the sets that we will consider for constructing a basis for $\mathrm{PRM}_d^{\sigma,\perp}(2)$.

If $M_a(d^\perp)$ contains monomials of the two types, then, besides T_a, Lemma C.3.10 states that there are more linearly independent polynomials in $\mathcal{T}(M_a(d^\perp))$. Thus, we turn our attention now to the case (4) from Lemma C.3.10. For each $a_2 \in \mathcal{A}^1$, let ξ_{a_2} be a primitive element in $\mathbb{F}_{q^{n_{a_2}}}$, and we consider the set

$$T_{a_2} = \{(x_0 - 1)(\mathcal{T}_{a_2}(\xi_{a_2}^r x_2^{a_2}) + \mathcal{T}_{a_2}(\xi_{a_2}^r)(x_1 - 1)) \mid 0 \leq r \leq n_{a_2} - 1\}.$$

Let $V = \{a_2 \in \mathcal{A}^1 \mid \mathfrak{I}_{a_2} \neq \mathfrak{I}_{\overline{d^\perp}}$ and $\exists\, c \in \mathcal{A}$ with $c_2 = a_2$ and $M_c(d^\perp)$ contains monomials of the two types$\}$, and we consider the set

$$D_2 = \bigcup_{a_2 \in V} T_{a_2}.$$

If we want to generate all the polynomials in $\bigcup_{a\in\mathcal{A}} \mathcal{T}(M_a(d^\perp))$, from Lemma C.3.10 we see that we still have to consider the polynomials corresponding to $a \in \mathcal{A}$ such that $\mathfrak{I}_{a_2} = \mathfrak{I}_{\overline{d}}$. Let us define a set D_3 that will contain the polynomials corresponding to this case and that we will consider for constructing a basis for $\mathrm{PRM}_d^{\sigma,\perp}(2)$. Let $a_2 \in \mathcal{A}^1$ such that $\mathfrak{I}_{a_2} = \mathfrak{I}_{\overline{d^\perp}}$, and ξ_{a_2} a primitive element in $\mathbb{F}_{q^{n_{a_2}}}$.

(a) If $M_{(0,\overline{d^\perp})}(d^\perp) = M_{(0,a_2)}(d^\perp)$ contains monomials of the two types:

(a.1) If there is an element $c \in \mathcal{A}$ such that $c_2 = a_2$, $\mathfrak{I}_c \neq \mathfrak{I}_{(0,\overline{d^\perp})}$, and $M_c(d^\perp)$ contains monomials of the two types, we set

$$D_3 = \{\mathcal{T}_{a_2}(\xi_{a_2}^r x_0 x_2^{a_2}) \mid 0 \leq r \leq n_{a_2} - 1\} \cup \{(x_0 - 1)(x_1 - 1)\}.$$

(a.2) We set

$$D_3 = \{\mathcal{T}_{a_2}(\xi_{a_2}^r x_0 x_2^{a_2}) \mid 0 \leq r \leq n_{a_2} - 1\}.$$

otherwise.

(b) We set

$$D_3 = \emptyset$$

otherwise.

We note that the case (b) happens if and only if x_0 does not divide any monomial in $M_{(0,\overline{d^\perp})}(d^\perp)$. The precise reason why we define D_3 in this way will be clear in the proof of Theorem C.3.12, which we will state after defining one last set, which we are considering just to cover the case in which $d \equiv 0 \bmod q^s - 1$. In that case, we also have the evaluation of 1 in the dual code of $\mathrm{PRM}_d(2)$ by Theorem C.3.2. If $d = q^s - 1$, we define $D_4 = \{1\}$, and $D_4 = \emptyset$ otherwise.

Theorem C.3.12. *Let $d \geq 1$ and $d^\perp = 2(q^s - 1) - d$. For each $a \in \mathcal{A}$, let ξ_a be a primitive element in $\mathbb{F}_{q^{n_a}}$ such that $\mathcal{T}_a(\xi_a) \neq 0$, and for each $a_2 \in \mathcal{A}^1$, let ξ_{a_2} be a primitive element in $\mathbb{F}_{q^{n_{a_2}}}$ such that $\mathcal{T}_{a_2}(\xi_{a_2}) \neq 0$ (one can always assume this [3]). Using the previous definitions, we consider the set*

$$D = D_1 \cup D_2 \cup D_3 \cup D_4.$$

Then we have that the image by the evaluation map of D forms a basis for $\mathrm{PRM}_d^{\sigma,\perp}(2)$.

Proof. Firstly, by Theorem C.3.2 we know that $\mathrm{PRM}_d^\perp(2)$ is equal to $\mathrm{PRM}_{d^\perp}(2)$, except when $d \equiv 0 \bmod (q^s - 1)$, in which case we also have to consider the evaluation of the constant 1. If $d \not\equiv 0 \bmod (q^s - 1)$, by Delsarte's Theorem, Theorem C.2.7, $\mathrm{PRM}_d^{\sigma,\perp}(2) = \mathrm{Tr}(\mathrm{PRM}_{d^\perp}(2))$, and due to the fact that we have $\mathrm{Tr} \circ \mathrm{ev} = \mathrm{ev} \circ \mathcal{T}$, we see that if we consider $\mathcal{T}(S_{d^\perp})$ (and possibly the constant 1), we obtain a system of generators for $\mathrm{PRM}_d^{\sigma,\perp}(2)$. Therefore, in order to obtain a basis, we just need to study linear independence between these polynomials. In fact, we have $S_{d^\perp} = \langle \bigcup_{a\in\mathcal{A}} M_a(d^\perp) \rangle$, which means that we can consider the union of the bases given for each $\mathcal{T}(M_a(d^\perp))$ from Lemma C.3.10, and we can obtain obtain a basis for $\mathrm{PRM}_d^{\sigma,\perp}(2)$ by extracting a maximal linearly independent set. We focus first on computing a basis for $\mathcal{T}(S_{d^\perp})$, and we will consider the cases where $d \equiv 0 \bmod q^s - 1$ later.

In what follows, for each $a \in \mathcal{A}$ we consider ξ_a a primitive element in $\mathbb{F}_{q^{n_a}}$, and for each $a_2 \in \mathcal{A}^1$ we consider ξ_{a_2} a primitive element in $\mathbb{F}_{q^{n_{a_2}}}$. By construction, it is clear that we have $D_1 \cup D_2 \subset \mathcal{T}(S_{d^\perp})$. We show now that also D_3 is contained in $\mathcal{T}(S_{d^\perp})$, and D_4 is contained in $\mathcal{T}(S_{d^\perp} + \langle 1 \rangle)$ when $D_4 \neq \emptyset$.

Let $a_2 \in \mathcal{A}^1$ such that $\mathfrak{I}_{a_2} = \mathfrak{I}_{\overline{d^\perp}}$. For D_3, we have to justify that, if $M_{(0,\overline{d^\perp})}(d^\perp)$ contains monomials of the two types and there is an element $c \in \mathcal{A}$ such that $c_2 = a_2$, $\mathfrak{I}_c \neq \mathfrak{I}_{(0,\overline{d^\perp})}$ and $M_c(d^\perp)$ contains monomials of the two types, then $(x_0 - 1)(x_1 - 1)$ is in $\mathcal{T}(S_{d^\perp})$. Under these assumptions, by Lemma C.3.10 we have that the following sets are in $\mathcal{T}(S_{d^\perp})$:

$$\begin{aligned}&\{\mathcal{T}_{(0,a_2)}(\xi_{(0,a_2)}^r x_2^{a_2}) \mid 0 \leq r \leq n_{(0,a_2)} - 1\} \cup \{\mathcal{T}_{(0,a_2)}(\xi_{(0,a_2)}^r x_0 x_2^{a_2}) \mid 0 \leq r \leq n_{(0,a_2)} - 1\},\\ &\{\mathcal{T}_c(\xi_a^r x_1^{c_1} x_2^{c_2}) \mid 0 \leq r \leq n_c - 1\}\\ &\qquad\qquad \cup \{(x_0 - 1)(\mathcal{T}_{c_2}(\xi_{c_2}^r x_2^{c_2}) + \mathcal{T}_{c_2}(\xi_{c_2}^r)(x_1 - 1)) \mid 0 \leq r \leq n_{c_2} - 1\}.\end{aligned} \tag{C.3.7}$$

Taking into account that $c_2 = a_2$, if we assume that $\xi_{(0,a_2)} = \xi_{a_2}$ (note that $n_{a_2} = n_{(0,a_2)}$), then $\mathcal{T}_{(0,a_2)}(\xi_{(0,a_2)}^r x_2^{a_2}) = \mathcal{T}_{c_2}(\xi_{c_2}^r x_2^{c_2})$ and $\mathcal{T}_{(0,a_2)}(\xi_{(0,a_2)}^r x_0 x_2^{a_2}) = x_0 \mathcal{T}_{c_2}(\xi_{c_2}^r x_2^{c_2})$. By assumption, we have that $\mathcal{T}_{c_2}(\xi_{c_2}) \neq 0$. Hence, taking into account that we can generate the polynomial $(1 - x_0)\mathcal{T}_{c_2}(\xi_{c_2} x_2^{c_2})$ with the first union of sets in (C.3.7), we see that with the first union of sets and the last set from (C.3.7) we can generate $(x_0 - 1)(x_1 - 1)$. Thus, $D_1 \cup D_2 \cup D_3 \subset \mathcal{T}(S_{d^\perp})$. On the other hand, if $d = q^s - 1$, we have $D_4 = \{1\}$, and it is clear that $D_4 \subset \mathcal{T}(S_{d^\perp} + \langle 1 \rangle)$. Therefore, we have seen that the image by the evaluation map of D is always in $\mathrm{PRM}_d^{\sigma,\perp}(2)$.

Now we justify that the evaluation of the polynomials in D is linearly independent. If we consider the monomials $x_0^{a_0} x_1^{a_1} x_2^{a_2}$, $x_0^{b_0} x_1^{b_1} x_2^{b_2}$, of degree $d^\perp$, with $\mathfrak{I}_a \neq \mathfrak{I}_b$ (for $a = (a_1, a_2)$, $b = (b_1, b_2)$), then we have that the sets $\{\mathcal{T}_a(\xi_a^r x_0^{a_0} x_1^{a_1} x_2^{a_2}), 0 \leq r \leq n_a - 1\}$ and $\{\mathcal{T}_b(\xi_b^r x_0^{b_0} x_1^{b_1} x_2^{b_2}), 0 \leq r \leq n_b - 1\}$ are linearly independent since in $[\{1\} \times \mathbb{F}_{q^s}^2]$ they are linearly independent by the affine case from Theorem C.2.3 in two variables. Using Lemma C.3.10 we see that the polynomials in D_1 are linearly independent.

Each polynomial $(x_0 - 1)(\mathcal{T}_{a_2}(\xi_{a_2}^r x_2^{a_2}) + \mathcal{T}_{a_2}(\xi_{a_2}^r)(x_1 - 1))$, with $0 \leq r \leq n_{a_2} - 1$, has the same evaluation in $[\{0\} \times \{1\} \times \mathbb{F}_{q^s}]$ as $-\mathcal{T}_{a_2}(\xi_{a_2}^r x_2^{a_2})$ in $\mathbb{F}_{q^s}$. Hence, the evaluation of the polynomials in D_2 is linearly independent by Theorem C.2.3 in one variable. Moreover, these polynomials evaluate to 0 in $[\{1\} \times \mathbb{F}_{q^s}^2]$, while the polynomials from D_1 have linearly independent evaluation in $[\{1\} \times \mathbb{F}_{q^s}^2]$, which means that the evaluation of $D_1 \cup D_2$ is also linearly independent.

We show now that a similar reasoning proves that the evaluation of $D_1 \cup D_2 \cup D_3$ is also linearly independent. Looking at the definition of D_3, if we are in the case (a.1), the evaluation of the polynomial $(x_0 - 1)(x_1 - 1)$ is linearly independent from the evaluation of the rest of polynomials in $D_1 \cup D_2 \cup D_3$ as it is the only one that evaluates to 0 in $[\{1\} \times \mathbb{F}_{q^s}^2]$ and $[\{0\} \times \{1\} \times \mathbb{F}_{q^s}]$, and the rest of polynomials have linearly independent evaluations in those sets. Let $a_2 \in \mathcal{A}^1$ such that $\mathfrak{I}_{a_2} = \mathfrak{I}_{\overline{d^\perp}}$. The evaluation of $\mathcal{T}_{a_2}(\xi_{a_2}^r x_0 x_2^{a_2})$, for some $0 \leq r \leq n_{a_2} - 1$, is linearly independent from the evaluation of any polynomial in D_1, besides $\mathcal{T}_{a_2}(\xi_{a_2}^r x_2^{a_2})$, due to the argument we used to discuss linear independence between elements in D_1. But its evaluation is also linearly independent from the evaluation of $\mathcal{T}_{a_2}(\xi_{a_2}^r x_2^{a_2})$ by Lemma C.3.10 (3). The same argument that we used to prove that the evaluation of the polynomials in $D_1 \cup D_2$ is linearly independent proves that the evaluation of $\mathcal{T}_{a_2}(\xi_{a_2}^r x_0 x_2^{a_2})$ is linearly independent from the evaluation of the polynomials in D_2.

Thus, in this case, the evaluation of $D_1 \cup D_2 \cup D_3$ is linearly independent. The same arguments prove that $D_1 \cup D_2 \cup D_3$ is linearly independent in the other cases that appear in the definition of D_3.

We study now the cases in which we have $D_4 \neq \emptyset$, i.e., the case where $d = q^s - 1$. The evaluation of the constant 1 is linearly independent from the evaluation of the rest of polynomials in this case since, if we look at the evaluation in $[\{0\} \times \{1\} \times \mathbb{F}_{q^s}]$, the constant 1 is linearly independent from the evaluation of the rest of univariate traces by Theorem C.2.3. Hence if we had a linear combination of polynomials from $D_1 \cup D_2 \cup D_3$ with the same evaluation as 1 in P^2, when setting $x_0 = 0, x_1 = 1$, the result would be the constant 1. If we look at the polynomials that we have in $D_1 \cup D_2 \cup D_3$, the only polynomial that would have a constant in its support after setting $x_0 = 0, x_1 = 1$, would be the only polynomial in T_0: $(x_0 - 1)(1 + (x_1 - 1)) = (x_0 - 1)x_1$. However, we only consider this polynomial in D_2 if there is some $b \in \mathcal{A}$ such that $\mathfrak{I}_{b_2} = \mathfrak{I}_0 = \{0\}$ and if $M_b(d^\perp) = M_b(q^s - 1)$ contains monomials of the two types. Therefore, $b_2 = 0$, and we must have $b_1 = q^s - 1$ if we want to have some monomial that is not divided by x_0 in $M_b(q^s - 1)$ by Lemma C.3.7. However, $M_{(q^s-1,0)}(q^s - 1) = \{x_1^{q^s-1}\}$ does not have monomials of the two types. Thus, the polynomial $(x_0 - 1)x_1$ is not in $D_1 \cup D_2 \cup D_3$ in this case and the evaluation of $D = D_1 \cup D_2 \cup D_3 \cup D_4$ is linearly independent.

The only thing left to prove for asserting that D is a basis is that this set is a maximal linearly independent set, or, equivalently, that D generates $\mathcal{T}(S_{d^\perp})$ if $d \not\equiv 0 \bmod q^s - 1$, and D generates $\mathcal{T}(S_{d^\perp} + \langle 1 \rangle)$ otherwise. To see that D generates $\mathcal{T}(S_{d^\perp})$ when $d \not\equiv 0 \bmod q^s - 1$, we have seen that it is enough to check that we can generate all the bases for the sets $\mathcal{T}(M_a(d^\perp))$ from Lemma C.3.10. Let $a \in \mathcal{A}$ such that $M_a(d^\perp) \neq \emptyset$. If $M_a(d^\perp)$ does not have monomials of the two types, then we see that the basis for $\mathcal{T}(M_a(d^\perp))$ from Lemma C.3.10 is contained in D_1. If $M_a(d^\perp)$ contains monomials of the two types, then we are in case (3) or case (4) from Lemma C.3.10.

Due to the ordering of the elements in $\mathbb{Z}_{q^s}^2$, $a \in \mathcal{A}$ implies that $a_2 \in \mathcal{A}^1$. We consider now the case (4) and we assume first that $\mathfrak{I}_{a_2} \neq \mathfrak{I}_{\overline{d^\perp}}$. In this situation, it is clear by the definitions that the basis for $\mathcal{T}(M_a(d))$ from Lemma C.3.10 is contained in $D_1 \cup D_2$.

Now we study the case (3) from Lemma C.3.10, and also the case (4) when $\mathfrak{I}_{a_2} = \mathfrak{I}_{\overline{d^\perp}}$, which are the only cases left. By Remark C.3.11, in both situations we have that $\mathfrak{I}_{a_2} = \mathfrak{I}_{\overline{d^\perp}}$. Instead of studying the sets $\mathcal{T}(M_c(d^\perp))$, with $c \in \mathcal{A}$ and $c_2 = a_2$, one by one, we consider them together in this case, and we will see that we can generate $\bigcup_{c \in \mathcal{A} | c_2 = a_2} \mathcal{T}(M_c(d^\perp))$. For each $c \in \mathcal{A}$ with $c_2 = a_2$ and $M_c(d^\perp) \neq \emptyset$, if $M_c(d^\perp)$ does not have monomials of the two types, we have already seen that the basis for $\mathcal{T}(M_c(d^\perp))$ from Lemma C.3.10 is contained in D_1. And if $M_c(d^\perp)$ contains monomials of the two types, then it is also clear that the first set of polynomials that appears in cases (3) and (4) from Lemma C.3.10 is contained in D_1. Thus, we focus on the second set of polynomials from those cases in Lemma C.3.10.

If $M_{(0,\overline{d^\perp})}(d^\perp) = M_{(0,a_2)}(d^\perp)$ contains monomials of the two types, by the definition of D_3 we have that the basis for $\mathcal{T}(M_{(0,a_2)}(d^\perp))$ from Lemma C.3.10 is contained in $D_1 \cup D_3$. If we also have some $c \in \mathcal{A}$, $\mathfrak{I}_c \neq \mathfrak{I}_{(0,a_2)}$, with $c_2 = a_2$, and such that $M_c(d^\perp)$ contains monomials of the two types, then we have that $(x_0 - 1)(x_1 - 1) \in D_3$, and by the reasoning that we did after (C.3.7) it is clear that we can generate the basis of $\mathcal{T}(M_c(d^\perp))$ given in Lemma C.3.10 with the polynomials in $D_1 \cup D_2 \cup D_3$.

If $M_{(0,a_2)}(d^\perp)$ does not have monomials of the two types, we clearly have the basis from

Lemma C.3.10 for $\mathcal{T}(M_{(0,a_2)}(d^\perp))$ contained in $D_1 \cup D_3$. We also note that, by Lemma C.3.7, $M_{(0,a_2)}(d^\perp)$ does not have monomials of the two types if and only if $d^\perp = a_2$, i.e., $d^\perp$ is the minimal element in $\mathfrak{I}_{d^\perp}$. Hence, for any $c \in \mathcal{A}$ with $c_2 = a_2 = d^\perp$, $\mathfrak{I}_c \neq \mathfrak{I}_{(0,d^\perp)}$, we obtain that, for each $\gamma \in \mathfrak{I}_c$, we have $\gamma_1 \neq 0$ and $\gamma_1 + \gamma_2 > c_2 = d^\perp$, which means that $M_c(d^\perp) = \emptyset$.

Finally, we have to consider the cases where $d \equiv 0 \bmod q^s - 1$. If $d = q^s - 1$, we already have $1 \in D_4$. For the case $d = 2(q^s - 1)$, we have $\mathcal{T}_{(0,0)}(x_1^0 x_2^0) = 1$ in D_1, which means that we also have the evaluation of the constant 1 when evaluating the polynomials in D. Therefore, we have proved that the image by the evaluation map of D is a basis for $\mathrm{PRM}_d^{\sigma,\perp}(2)$. □

Corollary C.3.13. *Let $d \geq 1$ and $d^\perp = 2(q^s-1)-d$. Let $U = \{a \in \mathcal{A} \mid M_a(d^\perp) \neq \emptyset\}$ and $V = \{a_2 \in \mathcal{A}^1 \mid \mathfrak{I}_{a_2} \neq \mathfrak{I}_{\overline{d^\perp}}$ and $\exists\ c \in \mathcal{A}$ with $c_2 = a_2$ and $M_c(d^\perp)$ contains monomials of the two types$\}$ as before. The dimension of $\mathrm{PRM}_d^{\sigma,\perp}(2)$ is*

$$\dim(\mathrm{PRM}_d^{\sigma,\perp}(2)) = |D| = |D_1| + |D_2| + |D_3| + |D_4| = \sum_{a \in U} n_a + \sum_{a_2 \in V} n_{a_2} + \epsilon_3 + \epsilon_4,$$

where $\epsilon_3 = n_{\overline{d^\perp}} + 1$ if $M_{(0,\overline{d^\perp})}(d^\perp)$ contains monomials of the two types and there is $\mathfrak{I}_c \neq \mathfrak{I}_{(0,\overline{d^\perp})}$ with $c_2 \in \mathfrak{I}_{\overline{d}}$ such that $M_c(d^\perp)$ contains monomials of the two types; $\epsilon_3 = n_{\overline{d^\perp}}$ if $M_{(0,\overline{d^\perp})}(d^\perp)$ contains monomials of the two types but there is no $\mathfrak{I}_c \neq \mathfrak{I}_{(0,\overline{d^\perp})}$ as before; and $\epsilon_3 = 0$ otherwise. Finally, $\epsilon_4 = |D_4|$, i.e., $\epsilon_4 = 1$ if $d = q^s - 1$, and $\epsilon_4 = 0$ otherwise.

Example C.3.14. Consider the extension $\mathbb{F}_4 \supset \mathbb{F}_2$ and let us compute the set D for $d = 4$. We have $d^\perp = 2$ and, from Example C.2.1, the set of minimal representatives is $\mathcal{A} = \{(0,0),(1,0),(0,1),(1,1),(3,0),(0,3),(3,3),(2,1),(1,3),(3,1)\}$. We start by constructing the set D_1. We consider the minimal representatives a such that $M_a(d^\perp) \neq \emptyset$, which by Lemma C.3.7 is equivalent to having $\mathfrak{I}_a \cap \Delta_{\leq d^\perp} \neq \emptyset$. The only cyclotomic sets that satisfy that condition in this case are $\mathfrak{I}_{(0,0)}$, $\mathfrak{I}_{(1,0)}$, $\mathfrak{I}_{(0,1)}$ and $\mathfrak{I}_{(1,1)}$. Therefore, we have $U = \{(0,0),(1,0),(0,1),(1,1)\}$ and $D_1 = \bigcup_{a \in U} T_a$. For example, assuming $\xi_{(1,0)}$ is a primitive element of $\mathbb{F}_4$, for $a = (1,0)$ we have

$$T_{(1,0)} = \{\mathcal{T}_{(1,0)}(\xi_{(1,0)}^r x_1) \mid 0 \leq r \leq 1\} = \{\xi_{(1,0)}^r x_1 + \xi^{2r} x_1^2 \mid 0 \leq r \leq 1\}.$$

We also have $|D_1| = \sum_{a \in U} n_a = 7$. For $|D_2|$, we consider $\mathcal{A}^1 = \{0,1,3\}$. The only $a \in \mathcal{A}$ such that $M_a(d^\perp)$ contains monomials of the two types are the ones such that $\mathfrak{I}_a \cap \Delta_{<d^\perp} \neq \emptyset$ and $\mathfrak{I}_a \cap (\Delta_{d^\perp} \cup \Delta_{\overline{d^\perp}}) \neq \emptyset$, according to Lemma C.3.7. This is a subset of U, and from the elements of U, the ones that satisfy this condition are $(1,0)$ and $(0,1)$. For example, $\mathfrak{I}_{(1,0)} \cap \Delta_{<2} = (1,0)$ and $\mathfrak{I}_{(1,0)} \cap \Delta_2 = (2,0)$. Hence, looking at the second coordinate of $(1,0)$ and $(0,1)$, we have $V = \{0,1\}$, and $D_2 = \bigcup_{a_2 \in V} T_{a_2}$. For example, if we consider $\xi_1 = \xi_{(1,0)}$ a primitive element of $\mathbb{F}_4$, for $a_2 = 1$ we have

$$\begin{aligned} T_1 =& \{(x_0 - 1)(\mathcal{T}_1(\xi_1^r x_2) + \mathcal{T}_1(\xi_1^r)(x_1 - 1)) \mid 0 \leq r \leq 1\} \\ =& \{(x_0 - 1)(\xi_1^r x_2 + \xi_1^{2r} x_2^2 + (\xi_1^r + \xi_1^{2r})(x_1 - 1)) \mid 0 \leq r \leq 1\}. \end{aligned}$$

We have $|D_2| = \sum_{a_2 \in V} n_{a_2} = 3$. One can check that $D_3 = D_4 = \emptyset$ in this case. Thus, the evaluation of the set $D_1 \cup D_2$ is a basis for $\mathrm{PRM}_4^{\sigma,\perp}(2)$, and $\dim \mathrm{PRM}_4^{\sigma,\perp}(2) = 10$.

C.3.2 Subfield subcodes of projective Reed-Muller codes

In this section we compute a basis for $\mathrm{PRM}_d^\sigma(2)$. The discussion gets more technical than in the previous case, but we can obtain explicit results as well. We start by considering some sets of polynomials that we use to construct a basis for the subfield subcode. We recall the notation $\mathcal{A}_{\leq d} = \{a \in \mathcal{A} \mid \mathfrak{I}_a \subset \Delta_{\leq d}\}$ and $\mathcal{A}_{<d} = \{a \in \mathcal{A} \mid \mathfrak{I}_a \subset \Delta_{<d}\}$. We also consider $\mathcal{A}^1_{\leq d} = \{a_2 \in \mathcal{A}^1 \mid \forall c_2 \in \mathfrak{I}_{a_2}, c_2 \leq d\}$ for the univariate case. It is also important to recall the definition of homogenized trace from (C.2.1).

Lemma C.3.15. *Let $1 \leq d \leq 2(q^s-1)$ and let ξ_a be a primitive element in $\mathbb{F}_{q^{n_a}}$. The image by the evaluation map of the polynomials in the set*

$$B_1 = \bigcup_{a \in \mathcal{A}_{<d}} \{x_0 \mathcal{T}_a(\xi_a^r x_1^{a_1} x_2^{a_2}) \mid 0 \leq r \leq n_a - 1\},$$

is in $\mathrm{PRM}_d^\sigma(2)$. Moreover, the evaluation of the polynomials in B_1 is linearly independent.

Proof. The evaluation of these polynomials in $[\{1\} \times \mathbb{F}_{q^s}^2]$ is the same as the evaluation of the polynomials of the set

$$\bigcup_{a \in \mathcal{A}_{<d}} \{\mathcal{T}_a(\xi_a^r x_1^{a_1} x_2^{a_2}) \mid 0 \leq r \leq n_a - 1\}$$

in $\mathbb{F}_{q^s}^2$. This set of polynomials evaluates to $\mathbb{F}_q$ by Theorem C.2.3, which means that the polynomials in B_1 evaluate to $\mathbb{F}_q$ in $[\{1\} \times \mathbb{F}_{q^s}^2]$, and they clearly evaluate to 0 in the rest of the points in P^2. By Lemma C.2.6, each of these polynomials evaluates to $\mathbb{F}_q$. We have to see that these polynomials are equivalent modulo $S/I(P^2)$ to some homogeneous polynomials of degree d, because in that case these polynomials would have the same evaluation as some homogeneous polynomials of degree d, which means that their evaluation is in $\mathrm{PRM}_d^\sigma(2)$. Let $a \in \mathcal{A}_{<d}$. For $0 \leq r \leq n_a - 1$, we consider the polynomial $\mathcal{T}_a^h(\xi_a^r x_1^{a_1} x_2^{a_2})$, where we homogenize up to degree d. Having $a \in \mathcal{A}_{<d}$ means that, after reducing the exponents modulo $q^s - 1$, the monomials $x_1^{c_1} x_2^{c_2}$ that appear in the support of $\mathcal{T}_a(\xi_a^r x_1^{a_1} x_2^{a_2})$ satisfy that $c_1 + c_2 < d$ (these exponents are precisely the elements of $\mathfrak{I}_a \subset \Delta_{<d}$). Therefore, after homogenizing up to degree d, x_0 divides all the monomials in the support of $\mathcal{T}_a^h(\xi_a^r x_1^{a_1} x_2^{a_2})$. Taking into account the equation $x_0^2 - x_0$ from $I(P^2)$, this means that $\mathcal{T}_a^h(\xi_a^r x_1^{a_1} x_2^{a_2}) \equiv x_0 \mathcal{T}_a(\xi_a^r x_1^{a_1} x_2^{a_2}) \bmod I(P^2)$ in this case. Hence, the evaluation of the polynomials in B_1 is in $\mathrm{PRM}_d^\sigma(2)$.

We finish the proof by noting that their evaluation is linearly independent precisely since their evaluation in $[\{1\} \times \mathbb{F}_{q^s}^2]$ is linearly independent by Theorem C.2.3. □

Example C.3.16. We consider an extension $\mathbb{F}_{16} \supset \mathbb{F}_2$ (i.e., $q = 2$, $s = 4$), and the goal of the examples in this section is to compute a basis for $\mathrm{PRM}_{21}^\sigma(2)$. We start by computing the set B_1, which is a set of linearly independent polynomials that evaluate to $\mathbb{F}_q$ by the previous discussion. First of all, we need to consider all the cyclotomic sets $\mathfrak{I}_a$ such that $\mathfrak{I}_a \subset \Delta_{<21}$. For each of those cyclotomic sets, we consider the corresponding set of traces from B_1. For example, we can consider the cyclotomic set $\mathfrak{I}_{(1,1)} = \{(1,1), (2,2), (4,4), (8,8)\}$, which gives us the following $n_{(1,1)} = 4$ polynomials (ξ

is a primitive element in $\mathbb{F}_{2^4}$):

$$\begin{aligned}
\mathcal{T}^h_{(1,1)}(x_1x_2) &= x_0^{19}x_1x_2 + x_0^{17}x_1^2x_2^2 + x_0^{13}x_1^4x_2^4 + x_0^5x_1^8x_2^8,\\
\mathcal{T}^h_{(1,1)}(\xi x_1x_2) &= \xi x_0^{19}x_1x_2 + \xi^2 x_0^{17}x_1^2x_2^2 + \xi^4 x_0^{13}x_1^4x_2^4 + \xi^8 x_0^5x_1^8x_2^8,\\
\mathcal{T}^h_{(1,1)}(\xi^2 x_1x_2) &= \xi^2 x_0^{19}x_1x_2 + \xi^4 x_0^{17}x_1^2x_2^2 + \xi^8 x_0^{13}x_1^4x_2^4 + \xi x_0^5x_1^8x_2^8,\\
\mathcal{T}^h_{(1,1)}(\xi^3 x_1x_2) &= \xi^3 x_0^{19}x_1x_2 + \xi^6 x_0^{17}x_1^2x_2^2 + \xi^{12} x_0^{13}x_1^4x_2^4 + \xi^9 x_0^5x_1^8x_2^8,
\end{aligned}$$

where we see that we are homogenizing up to degree $d = 21$. As we have said in the previous discussion, these polynomials are linearly independent because in $[\{1\} \times \mathbb{F}_{q^s}^2]$ they have the same evaluation as the traces $\mathcal{T}_{(1,1)}(\xi^r x_1x_2)$, $0 \leq r \leq n_{(1,1)} - 1$, that would appear in the affine case from Theorem C.2.3. And they clearly evaluate to $\mathbb{F}_q$, as they evaluate to 0 in the rest of the points of P^2. We can continue doing this for all the other cyclotomic sets such that $\mathfrak{I}_a \subset \Delta_{<21}$, and we obtain $\sum_{a\in\mathcal{A}_{<21}} n_a = 127$ linearly independent polynomials that form B_1.

We consider now another set of homogeneous polynomials that will be linearly independent from B_1 and whose polynomials evaluate to $\mathbb{F}_q$. We start with the case $d \leq q^s - 1$, which is easier. Let us focus first on the cyclotomic sets $\mathfrak{I}_a$ with $a \in \mathcal{A}_{\leq d} \setminus \mathcal{A}_{<d}$. Having $\mathfrak{I}_a \cap \Delta_d \neq \emptyset$ implies that the corresponding homogeneous traces $\mathcal{T}^h_a(\xi_a^r x_1^{a_1} x_2^{a_2})$, $0 \leq r \leq n_a - 1$, with ξ_a a primitive element in $\mathbb{F}_{q^{n_a}}$, have at least one monomial which is not divisible by x_0. Hence, although the evaluation of these traces in $[\{1\} \times \mathbb{F}_{q^s}^2]$ is going to be equal to the evaluation of $\mathcal{T}_a(\xi_a^r x_1^{a_1} x_2^{a_2})$ in $\mathbb{F}_{q^s}^2$, which has coordinates in $\mathbb{F}_q$, the evaluation in $[\{0\} \times \{1\} \times \mathbb{F}_{q^s}]$ and $[0 : 0 : 1]$ does not necessarily have its coordinates in $\mathbb{F}_q$, and, by Lemma C.2.6, these polynomials might not evaluate to $\mathbb{F}_q$. By Lemma C.2.6 and Theorem C.2.3 in one variable, if a polynomial $f(x_0, x_1, x_2)$ evaluates to $\mathbb{F}_q$ in P^2, $f(0, 1, x_2)$ must be a linear combination of traces in the variable x_2. A natural idea is to consider linear combinations of homogenized traces such that, when setting $x_0 = 0, x_1 = 1$, we obtain that the evaluation of $f(0, 1, x_2)$ in $\mathbb{F}_{q^s}$ is the same as some trace in the variable x_2. To do that, we introduce the following definition.

Definition C.3.17. For each $a_2 \in \mathcal{A}^1_{\leq d}$, we define the set

$$Y_{a_2} := \{a \in \mathcal{A}_{\leq d} \mid \mathfrak{I}_a = \mathfrak{I}_{(\overline{d-c_2},c_2)} \text{ for some } c_2 \in \mathfrak{I}_{a_2}\}.$$

Remark C.3.18. Recall that, with the order chosen for the cyclotomic sets, we have that $c \in \mathcal{A}$ implies $c_2 \in \mathcal{A}^1$. Therefore, in this case $c \in Y_{a_2}$ implies $c_2 = a_2$.

Example C.3.19. Let us continue with the setting of Example C.3.16. We have $d = 21$ and $\overline{d} = 6$, and we will compute Y_{a_2} for $a_2 = 0, 1$. To do so, we consider first the univariate cyclotomic sets:

$$\mathfrak{I}_0 = \{0\}, \mathfrak{I}_1 = \{1, 2, 4, 8\}, \mathfrak{I}_3 = \{3, 6, 9, 12\}, \mathfrak{I}_5 = \{5, 10\}, \mathfrak{I}_7 = \{7, 11, 13, 14\}, \mathfrak{I}_{15} = \{15\}.$$

For $a_2 = 0$, we just have $Y_0 = \{(3, 0)\}$ because $\mathfrak{I}_{(3,0)} = \mathfrak{I}_{(6,0)} = \mathfrak{I}_{(\overline{d-0},0)}$. For $a_2 = 1$, we need to obtain the minimal elements of the cyclotomic sets $\mathfrak{I}_{(\overline{21-1},1)}, \mathfrak{I}_{(\overline{21-2},2)}, \mathfrak{I}_{(\overline{21-4},4)}$

and $\mathfrak{I}_{(21-8,8)}$. We have

$$\begin{aligned}\mathfrak{I}_{(5,1)} &= \{(5,1),(10,2),(5,4),(10,8)\},\\ \mathfrak{I}_{(4,2)} &= \{(2,1),(4,2),(8,4),(1,8)\},\\ \mathfrak{I}_{(2,4)} &= \{(8,1),(1,2),(2,4),(4,8)\},\\ \mathfrak{I}_{(13,8)} &= \{(11,1),(7,2),(14,4),(13,8)\}.\end{aligned}$$

Hence, $Y_1 = \{(2,1),(5,1),(8,1),(11,1)\}$.

The idea behind the definition of Y_{a_2} is the following: if we consider $c \in Y_{a_2}$ and the polynomial $\mathcal{T}_c^h(\xi_c^r x_1^{c_1} x_2^{c_2})$, then, if $\overline{d-c_2} = d - c_2$, we have the monomial $x_1^{d-c_2}x_2^{c_2}$ in the support of this homogenized trace (if $\overline{d-c_2} < d-c_2$, we would have the monomial $x_0^{q^s-1}x_1^{\overline{d-c_2}}x_2^{c_2}$ instead), and when setting $x_0 = 0$ and $x_1 = 1$, we obtain the monomial $x_2^{c_2}$, with $c_2 \in \mathfrak{I}_{a_2}$, in the support of $f(0,1,x_2)$. We have

$$\overline{d-c_2} = d - c_2 \iff d - c_2 \leq q^s - 1 \iff d - (q^s-1) \leq c_2. \tag{C.3.8}$$

In fact, it is clear that all the monomials that we obtain from this homogenized trace when setting $x_0 = 0, x_1 = 1$, are monomials $x_2^{c_2}$ with $c_2 \in \mathfrak{I}_{a_2}$. Thus, the traces associated to $c \in Y_{a_2}$ give monomials $x_2^{c_2}$ with $c_2 \in \mathfrak{I}_{a_2}$ when setting $x_0 = 0, x_1 = 1$.

The case with $\mathfrak{I}_{a_2} = \mathfrak{I}_{\overline{d}}$ is slightly more complicated, since in this case we have two monomials, $x_1^{q^s-1}x_2^{\overline{d}}$ and x_2^d (if $d \geq q^s$), of degree d with different evaluation in P^2 which give the same monomial $x_2^{\overline{d}}$ when setting $x_0 = 0, x_1 = 1$. This means that two different homogenized traces from different cyclotomic sets can have $x_2^{\overline{d}}$ in its support. We will exclude this case in what follows now as we will study this case separately later. Hence, for a given $a_2 \in \mathcal{A}^1_{\leq d}$ with $\mathfrak{I}_{a_2} \neq \mathfrak{I}_{\overline{d}}$ and ξ_{a_2} a primitive element in $\mathbb{F}_{q^{n_{a_2}}}$, we can consider the sum

$$f_{a_2}^r = \sum_{c \in Y_{a_2}} \mathcal{T}_c^h(\xi_{a_2}^r x_1^{c_1} x_2^{c_2}),$$

for $0 \leq r \leq n_{a_2}$, and, due to the previous discussion, we obtain that in the support of $f_{a_2}^r(0,1,x_2)$ there are only monomials of the form $x_2^{\gamma_2}$ with $\gamma_2 \in \mathfrak{I}_{a_2}$. Each monomial $x_2^{\gamma_2}$ can only come from one of the homogenized traces since, if $\gamma_2 \neq \overline{d}$, this monomial can only come from the monomial $x_1^{d-\gamma_2}x_2^{\gamma_2}$ in the support of $f_{a_2}^r$, with $\gamma_2 \geq d - (q^s-1)$ due to (C.3.8). Moreover, the coefficient of each of these monomials $x_2^{\gamma_2}$ is the same that this monomial would have in $\mathcal{T}_{a_2}(\xi_{a_2}^r x_2^{a_2})$ because we saw in Remark C.3.18 that $c_2 = a_2$ for every $c \in Y_{a_2}$. If $d \leq q^s - 1$, the condition from Equation (C.3.8) is always satisfied for any $\gamma_2 \in \mathfrak{I}_{a_2}$. In this case, if we have

$$\bigcup_{c_2 \in \mathfrak{I}_{a_2}} \mathfrak{I}_{(d-c_2,c_2)} \subset \Delta_{\leq d},$$

then Y_{a_2} contains all the minimal elements $\gamma \in \mathcal{A}$ such that $\mathfrak{I}_\gamma = \mathfrak{I}_{(d-\gamma_2,\gamma_2)}$. Therefore, we have all the monomials $x_1^{d-\gamma_2}x_2^{\gamma_2}$, for $\gamma_2 \in \mathfrak{I}_{a_2}$, in the support of $f_{a_2}^r$, and we obtain $f_{a_2}^r(0,1,x_2) = \mathcal{T}_{a_2}(\xi_{a_2}^r x_2^{a_2})$. The polynomials $f_{a_2}^r$ are homogeneous of degree d and, by Lemma C.2.6, they evaluate to $\mathbb{F}_q$. Thus, their evaluation is in $\mathrm{PRM}_d^\sigma(2)$.

For $d \geq q^s$, we can consider instead the condition

$$\bigcup_{c_2 \in \mathfrak{I}_{a_2}, c_2 > d-(q^s-1)} \mathfrak{I}_{(d-c_2,c_2)} \subset \Delta_{\leq d}. \tag{C.3.9}$$

We avoid the case $c_2 = d-(q^s-1) = \overline{d}$ as we will study it later, and we consider only $c_2 > d-(q^s-1)$ in order to satisfy Equation (C.3.8). Reasoning as in the previous case, if the previous condition is satisfied, then $f^r_{a_2}(0,1,x_2)$ has in its support all the terms from $\mathcal{T}_{a_2}(\xi^r_{a_2}x_2^{a_2})$ with degree greater than $d-(q^s-1) = \overline{d}$. We claim that, in this situation, it is always possible to construct a polynomial $g^r_{a_2}$ whose evaluation is in $\mathrm{PRM}^\sigma_d(2)$ and such that $g^r_{a_2}(1,x_1,x_2) = f^r_{a_2}(1,x_1,x_2)$, $g^r_{a_2}(0,1,x_2) = \mathcal{T}_{a_2}(\xi^r_{a_2}x_2^{a_2})$, and $g^r_{a_2}(0,0,1) = 0$.

We first note that, in this situation, we can homogenize the equations of the field and obtain homogeneous polynomials of degree d. By this, what we mean is that we can consider a multiple of $x_i^{q^s} - x_i$, for $i = 1, 2$, and homogenize it up to degree d. If this multiple has degree less than d, then that homogenized polynomial evaluates to the 0 vector in P^2. However, when the degree of this multiple is exactly equal to $d \geq q^s$, we can obtain the following polynomials by multiplying the field equations by monomials and then homogenizing:

$$\left(x_1^{c_1}x_2^{c_2-1}(x_2^{q^s} - x_2)\right)^h = \left(x_1^{c_1}x_2^{c_2+q^s-1} - x_1^{c_1}x_2^{c_2}\right)^h = x_1^{c_1}x_2^{c_2+q^s-1} - x_0^{q^s-1}x_1^{c_1}x_2^{c_2},$$

where we are assuming that $c_1+c_2+q^s-1 = d$ and $c_2 > 0$. We note that we only consider $d \leq 2(q^s-1)$ (for a higher degree $\mathrm{PRM}_d(2)$ is the whole space). Thus, $c_1 + c_2 = \overline{d}$. Using the other field equation, we can get

$$\left(x_1^{c_1-1}x_2^{c_2}(x_1^{q^s} - x_1)\right)^h = \left(x_1^{c_1+q^s-1}x_2^{c_2} - x_1^{c_1}x_2^{c_2}\right)^h = x_1^{c_1+q^s-1}x_2^{c_2} - x_0^{q^s-1}x_1^{c_1}x_2^{c_2},$$

All of these polynomials are equivalent to $x_1^{c_1}x_2^{c_2}(1-x_0)$ in $S/I(P^2)$, which is a more compact way of writing them, and we will refer to them as *homogenized field equations*. Although this last expression is not homogeneous, it has the same evaluation in P^2 as a homogeneous polynomial of degree d, which implies that its evaluation is also in $\mathrm{PRM}_d(2)$. With this in mind, we have that, for any $0 \leq c_2 \leq \overline{d}-1$, the polynomial $x_1^{\overline{d}-c_2}x_2^{c_2}(1-x_0)$ can be seen as a homogeneous polynomial of degree d, and its evaluation in $[\{1\} \times \mathbb{F}^2_{q^s}]$ is the zero vector, in $[\{0\} \times \{1\} \times \mathbb{F}_{q^s}]$ it is the same as the evaluation of $x_2^{c_2}$, and it is 0 in $[0:0:1]$. Moreover, the polynomial $x_1x_2^{c_2}(1-x_0)$ has the same evaluation. For $c_2 = \overline{d}$, we have the polynomial $x_2^{\overline{d}}(1-x_0)$, but in this case the evaluation at $[0:0:1]$ of this polynomial is equal to 1. This polynomial will only be considered later when we study the case with $\mathfrak{I}_{a_2} = \mathfrak{I}_{\overline{d}}$.

As a consequence, if we add to $f^r_{a_2}$ a homogenized field equation, the evaluation of the resulting polynomial in $[\{1\} \times \mathbb{F}^2_{q^s}]$ does not change, and when setting $x_0 = 0, x_1 = 1$, we obtain $f^r_{a_2}(0,1,x_2) + x_2^{c_2}$, for some $0 \leq c_2 \leq \overline{d}-1$. Hence, if $\mathfrak{I}_{a_2} \neq \mathfrak{I}_{\overline{d}}$, and if we have the condition $\bigcup_{c_2 \in \mathfrak{I}_{a_2}, c_2 > d-(q^s-1)} \mathfrak{I}_{(d-c_2,c_2)} \subset \Delta_{\leq d}$ (we recall that, under this assumption, $f^r_{a_2}(0,1,x_2)$ has in its support all the terms from $\mathcal{T}_{a_2}(\xi^r_{a_2}x_2^{a_2})$ with degree greater than $\overline{d}$), then, adding adequate multiples of the homogenized field equations, we can obtain a polynomial $g^r_{a_2}$ such that $g^r_{a_2}(1,x_1,x_2) = f^r_{a_2}(1,x_1,x_2)$, $g^r_{a_2}(0,1,x_2) = \mathcal{T}_{a_2}(\xi^r_{a_2}x_2^{a_2})$, and $g^r_{a_2}(0,0,1) = 0$. Therefore, the polynomial $g^r_{a_2}$ is defined as the polynomial obtained

by adding the necessary multiples of the homogenized field equations to $f^r_{a_2}$ to obtain $g^r_{a_2}(0,1,x_2) = \mathcal{T}_{a_2}(\xi^r_{a_2}x_2^{a_2})$. Because of all the previous discussion, it is clear that the evaluation of $g^r_{a_2}$ is in $\mathrm{PRM}^\sigma_d(2)$.

Moreover, we see that the polynomial

$$h^r_{a_2} = x_0\left(\sum_{c\in Y_{a_2}} \mathcal{T}_c(\xi^r_{a_2}x_1^{c_1}x_2^{c_2})\right) + (1-x_0)x_1\mathcal{T}_{a_2}(\xi^r_{a_2}x_2^{a_2})$$

has the same evaluation as the polynomial $g^r_{a_2}$, which means that its evaluation is also in $\mathrm{PRM}^\sigma_d(2)$.

Furthermore, avoiding the case in which $\mathfrak{I}_{a_2} = \mathfrak{I}_{\overline{d}}$, we can express both the case with $d \geq q^s$ and $d \leq q^s - 1$ using the same polynomials and conditions. To see this, we first introduce the following notation:

$$Y = \left\{ a_2 \in \mathcal{A}^1_{\leq d} \mid \mathfrak{I}_{a_2} \neq \mathfrak{I}_{\overline{d}} \text{ such that } \bigcup_{c_2\in\mathfrak{I}_{a_2}, c_2 > d-(q^s-1)} \mathfrak{I}_{(d-c_2,c_2)} \subset \Delta_{\leq d} \right\}.$$

The elements of Y are just the $a_2 \in \mathcal{A}^1_{\leq d}$ such that we can construct a polynomial in $\mathrm{PRM}^\sigma_d(2)$ whose evaluation in $[\{0\}\times\{1\}\times\mathbb{F}_{q^s}]$ is equal to some trace of $x_2^{a_2}$ with the previous ideas. In the case $d \leq q^s - 1$, the condition in the set Y is the same that we were considering before. Note that for $a_2 = 0$ and $d = q^s - 1$, the condition that we had for $d \leq q^s - 1$ was

$$\bigcup_{c_2\in\mathfrak{I}_{a_2}} \mathfrak{I}_{(d-c_2,c_2)} = \mathfrak{I}_{(q^s-1,0)} = \{(q^s-1,0)\} \subset \Delta_{\leq q^s-1},$$

which is always satisfied. The condition that we have used for Y when $a_2 = 0$ and $d = q^s-1$ would be

$$\bigcup_{c_2\in\mathfrak{I}_{a_2}, c_2 > d-(q^s-1)} \mathfrak{I}_{(d-c_2,c_2)} = \emptyset \subset \Delta_{\leq d},$$

which is always satisfied as well. The following result summarizes the previous discussion.

Lemma C.3.20. *Let $1 \leq d \leq 2(q^s-1)$, and let ξ_{a_2} be a primitive element in $\mathbb{F}_{q^{n_{a_2}}}$. The evaluation of the polynomials in the set*

$$B_2 = \bigcup_{a_2\in Y}\left\{ x_0\left(\sum_{c\in Y_{a_2}} \mathcal{T}_c(\xi^r_{a_2}x_1^{c_1}x_2^{c_2})\right) + (1-x_0)x_1\mathcal{T}_{a_2}(\xi^r_{a_2}x_2^{a_2}), 0 \leq r \leq n_{a_2}-1 \right\}$$

is in $\mathrm{PRM}^\sigma_d(2)$. Moreover, the evaluation of the polynomials in $B_1 \cup B_2$ is linearly independent.

Proof. In the previous discussion we have showed that, if $d \geq q^s$, all the polynomials in B_2 have their evaluation in $\mathrm{PRM}_d(2)$, and we also checked that they evaluate to $\mathbb{F}_q$ due to Lemma C.2.6. For the case $d \leq q^s - 1$, these polynomials have the same evaluation as $f^r_{a_2}$, which means that their evaluation is also in $\mathrm{PRM}^\sigma_d(2)$.

The evaluation of the polynomials in B_2 is linearly independent since it is linearly independent in $[\{0\}\times\{1\}\times\mathbb{F}_{q^s}]$ by the affine case from Theorem C.2.3: in $[\{0\}\times\{1\}\times\mathbb{F}_{q^s}]$

we have univariate traces in x_2 from different cyclotomic sets. Moreover, the evaluation of the polynomials in B_2 is linearly independent from the evaluation of the polynomials in B_1 because the evaluation of the polynomials in B_1 is zero in $[\{0\} \times \{1\} \times \mathbb{F}_{q^s}]$. □

Remark C.3.21. Let $a_2 \in \mathcal{A}^1$, and let

$$Y'_{a_2} := \{a \in \mathcal{A}_{\leq d} \setminus \mathcal{A}_{<d} \mid \mathfrak{I}_a = \mathfrak{I}_{(\overline{d-c_2},c_2)} \text{ for some } c_2 \in \mathfrak{I}_{a_2}\}.$$

The set

$$B'_2 = \bigcup_{a_2 \in Y} \left\{ x_0 \left(\sum_{c \in Y'_{a_2}} \mathcal{T}_c(\xi_{a_2}^r x_1^{c_1} x_2^{c_2}) \right) + (1-x_0) x_1 \mathcal{T}_{a_2}(\xi_{a_2}^r x_2^{a_2}), 0 \leq r \leq n_{a_2} - 1 \right\}$$

has the same properties as B_2 in Lemma C.3.20. This is because, for any $a \in \mathcal{A}_{<d}$, we have already considered $x_0\mathcal{T}_a(\xi_a^r x_1^{a_1} x_2^{a_2})$, $0 \leq r \leq n_a - 1$, in B_1, and $x_0\mathcal{T}_a(\xi_{a_2}^r x_1^{a_1} x_2^{a_2})$ is in the span of those traces for any $0 \leq r \leq n_{a_2} - 1$.

Example C.3.22. Let us continue with the setting from Example C.3.19 and compute the polynomials in the set B'_2 defined in Remark C.3.21, although we will also compute all the sets needed to obtain B_2 as well. We first compute Y. We have that $a_2 \in Y$ if the condition (C.3.9) is verified. In this case, $d = 21$ and $d - (q^s - 1) = \overline{d} = 6$. For $a_2 = 0$ we have $\mathfrak{I}_0 = \{0\}$, and the union of cyclotomic sets in the left hand side of (C.3.9) is empty, which means that the condition is satisfied, and $0 \in Y$.

For $a_2 = 1$, we verify that $\{(11,1),(7,2),(13,8),(14,4)\} = \mathfrak{I}_{(21-8,8)} \subset \Delta_{\leq 21}$ (note that 8 is the only element in $\mathfrak{I}_1$ greater than $\overline{d} = 6$). The condition (C.3.9) is satisfied and $1 \in Y$. We do not consider $a_2 = 3$ now since $\mathfrak{I}_3 = \mathfrak{I}_{\overline{d}}$, which is the case that we will cover in Example C.3.25. For $a_2 \in \{5, 7, 15\}$, it is easy to check that we have $a_2 \notin Y$. For example, for $a_2 = 7$, the cyclotomic set $\mathfrak{I}_{(21-7,7)} = \{(14,7),(7,11),(11,13),(13,14)\} \not\subset \Delta_{\leq 21}$, because, for instance, $(11,13) \notin \Delta_{\leq 21}$. Therefore, we have

$$Y = \{0, 1\}.$$

Now, for each $a_2 \in Y$, we have to compute Y_{a_2}. This was already done in Example C.3.19, and $Y_0 = \{(3,0)\}$ and $Y_1 = \{(2,1),(5,1),(8,1),(11,1)\}$. By Remark C.3.21, we can consider the sets $Y'_0 = \emptyset$ and $Y'_1 = \{(11,1)\}$ ($\mathfrak{I}_{(11,1)}$ is the only cyclotomic set that we have considered which is in $\Delta_{\leq 21} \setminus \Delta_{<21}$) instead of Y_0, Y_1, respectively, and the set B'_2 obtained satisfies the same properties as B_2. For simplicity, we construct B'_2 instead of B_2.

We now obtain the polynomials in B'_2. For $a_2 = 0$ we have $n_{a_2} = n_0 = 1$, which means that we only consider one polynomial, and we also have $Y'_0 = \emptyset$. We consider the following polynomial:

$$\{(1-x_0)x_1\mathcal{T}_0(x_2^0)\} = \{(1-x_0)x_1\}.$$

For the case $a_2 = 1$, we have $n_{a_2} = n_1 = 4$, and we have $Y'_1 = \{(11,1)\}$. Thus, using Remark C.3.21, we consider the set of polynomials

$$\{x_0\mathcal{T}_{(11,1)}(\xi_1^r x_1^{11} x_2) + (1-x_0)x_1\mathcal{T}_1(\xi_1^r x_2), 0 \leq r \leq n_1 - 1\},$$

where ξ_1 is a primitive element in $\mathbb{F}_{q^{n_1}} = \mathbb{F}_{16}$. Hence, we have constructed the set

$$B_2' = \{(1-x_0)x_1\} \cup \{x_0\mathcal{T}_{(11,1)}(\xi_1^r x_1^{11} x_2) + (1-x_0)x_1\mathcal{T}_1(\xi_1^r x_2), 0 \leq r \leq n_1 - 1\},$$

whose size is $n_1 + n_0 = 5$. In Example C.3.16 we obtained that the cardinality of B_1 is 127. This means that $B_1 \cup B_2'$ (and $B_1 \cup B_2$) contains 132 polynomials whose evaluation is in $\mathrm{PRM}_{21}^{\sigma}(2)$, and the evaluation of these polynomials is linearly independent.

We construct now one last set B_3. In the previous study, we have omitted the case in which $\mathfrak{I}_{a_2} = \mathfrak{I}_{\overline{d}}$. Therefore, we consider now $a_2 \in \mathcal{A}^1$ be such that $\mathfrak{I}_{a_2} = \mathfrak{I}_{\overline{d}}$. We assume that $a_2 \in \mathcal{A}^1_{\leq d}$ (if $a_2 \notin \mathcal{A}^1_{\leq d}$ the set B_3 will be the empty set). We follow a very similar reasoning to the one we did for the set B_2. For the case $1 \leq d \leq q^s - 1$, we were considering the polynomials

$$f_{a_2}^r = \sum_{c \in Y_{a_2}} \mathcal{T}_c^h(\xi_{a_2}^r x_1^{c_1} x_2^{c_2})$$

to construct B_2. We can still consider such a polynomial if $\mathfrak{I}_{a_2} = \mathfrak{I}_d$, but in this case, $f_{a_2}^r(0,0,1)$ is the coefficient of x_2^d in $f_{a_2}^r$, which is nonzero if $\mathfrak{I}_{(0,d)} \subset \Delta_{\leq d}$. We have that $f_{a_2}^r(0,0,1) \in \mathbb{F}_q$ only if $r = 0$, and in that case the polynomial

$$l_{a_2} = x_0 \left(\sum_{c \in Y_{a_2}} \mathcal{T}_c(x_1^{c_1} x_2^{c_2}) \right) + (1-x_0)x_1\mathcal{T}_{a_2}(x_2^{a_2}) + (1-x_0)(1-x_1)x_2^d$$

has the same evaluation in P^2 as $f_{a_2}^0$. If $\bigcup_{c_2 \in \mathfrak{I}_{a_2}} \mathfrak{I}_{(d-c_2,c_2)} \subset \Delta_{\leq d}$, i.e., we have $f_{a_2}^0(0,1,x_2) = \mathcal{T}_{a_2}(x_2^{a_2}) = \mathcal{T}_d(x_2^d)$, l_{a_2} evaluates to $\mathbb{F}_q$ and its evaluation is in $\mathrm{PRM}_d(2)$ (it has the same evaluation as $f_{a_2}^r$).

For the case $d \geq q^s$, we can consider the homogenized field equation $x_2^{\overline{d}}(1-x_0)$ to obtain a polynomial $g_{a_2}^r$ such that $g_{a_2}^r(1,x_1,x_2) = f_{a_2}^r(1,x_1,x_2)$ and $g_{a_2}^r(0,1,x_2) = \mathcal{T}_{a_2}(\xi_{a_2}^r x_2^{a_2})$. The problem that arises in this specific case is the following: the monomial $x_2^{\overline{d}}$ can be obtained when setting $x_0 = 0, x_1 = 1$, from the monomials $x_1^{q^s-1}x_2^{\overline{d}}$ and x_2^d, both of them of degree d. Hence, following the previous notation, we have to study two different cases: if $f_{a_2}^r(0,1,x_2)$ has $x_2^{\overline{d}}$ in its support (which means that $x_1^{q^s-1}x_2^{\overline{d}}$ is in the support of f), or if $f_{a_2}^r(0,1,x_2)$ does not have $x_2^{\overline{d}}$ in its support.

We start with the case in which $f_{a_2}^r(0,1,x_2)$ does not have $x_2^{\overline{d}}$ in its support, where we need to use $x_2^{\overline{d}}(1-x_0)$ to construct $g_{a_2}^r$. The main difference is that in this case $g_{a_2}^r(0,0,1)$ is equal to the coefficient of $x_2^{\overline{d}}$, which is nonzero. Therefore, by Lemma C.2.6, this coefficient has to be in $\mathbb{F}_q$ if $g_{a_2}^r$ evaluates to $\mathbb{F}_q$. We are also interested in obtaining $g_{a_2}^r(0,1,x_2) = \mathcal{T}_{a_2}(\xi_{a_2}^r x_2^{a_2})$ for some $0 \leq r \leq n_{a_2} - 1$. The coefficient of $x_2^{\overline{d}}$ in $g_{a_2}^r(0,1,x_2)$ is precisely the coefficient with which we considered $x_2^{\overline{d}}(1-x_0)$ when constructing $g_{a_2}^r$. Thus, the only possibility to have this coefficient in $\mathbb{F}_q$ is that this coefficient is equal to 1 (the case $r = 0$), and $g_{a_2}^0(0,1,x_2) = \mathcal{T}_{a_2}(x_2^{a_2})$. With this in mind, it is easy to check that l_{a_2}, as defined previously, has the same evaluation as the polynomial $g_{a_2}^0$ in P^2 in this case. As we argued for the set B_2, to ensure that the evaluation of l_{a_2} is in $\mathrm{PRM}_d(2)$, we need to have $\bigcup_{c_2 \in \mathfrak{I}_{a_2}, c_2 > d-(q^s-1)} \mathfrak{I}_{(d-c_2,c_2)} \subset \Delta_{\leq d}$. This condition ensures that $f_{a_2}^0(0,1,x_2)$ has all the monomials from $\mathcal{T}_{a_2}(x_2^{a_2})$ in its support, except maybe the monomials $x_2^{c_2}$ with

$c_2 \in \{0, 1, \ldots, \overline{d}\}$, which appear in the support of $g^0_{a_2}(0, 1, x_2)$ when adding to $f^0_{a_2}(0, 1, x_2)$ the corresponding homogenized field equations.

Finally, we consider the case in which we have $x_1^{q^s-1}x_2^{\overline{d}}$ in the support of $f^r_{a_2}$, i.e., $f^r_{a_2}(0, 1, x_2)$ has $x_2^{\overline{d}}$ in its support. If we look at the definition of $f^r_{a_2}$, this happens if and only if $\mathfrak{I}_{(q^s-1,\overline{d})} \subset \Delta_{\leq d}$. This is equivalent to having that $\overline{d}$ is the maximal element of $\mathfrak{I}_{a_2}$. Therefore, the condition $\bigcup_{c_2 \in \mathfrak{I}_{a_2}, c_2 > d-(q^s-1)} \mathfrak{I}_{(d-c_2,c_2)} = \emptyset \subset \Delta_{\leq d}$ is automatically satisfied in this case. This allows us to construct a polynomial l'_{a_2} which is very similar to l_{a_2}:

$$l'_{a_2} = l_{a_2} - x_0 \mathcal{T}_{(q^s-1,a_2)}(x_1^{q^s-1}x_2^{a_2}).$$

Indeed, we can subtract the polynomial $\mathcal{T}^h_{(q^s-1,\overline{d})}(x_1^{c_1}x_2^{c_2})$ from $f^0_{a_2}$, and, adding the corresponding homogenized field equations (we will need to use $x_2^{\overline{d}}(1 - x_0)$ in order to obtain $\mathcal{T}_{a_2}(x_2^{a_2})$ when setting $x_0 = 0, x_1 = 1$, as we have subtracted the monomial $x_1^{q^s-1}x_2^{\overline{d}}$), we would get a polynomial g'_{a_2} such that $g'_{a_2}(1, x_1, x_2) = f^0_{a_2}(1, x_1, x_2) - \mathcal{T}_{(q^s-1,a_2)}(x_1^{q^s-1}x_2^{a_2})$, $g'_{a_2}(0, 1, x_2) = \mathcal{T}_{a_2}(x_2^{a_2})$, $g'_{a_2}(0, 0, 1) = 1$. Hence, the polynomial l'_{a_2} has the same evaluation as the polynomial g'_{a_2}, which means that the evaluation of l'_{a_2} is in $\mathrm{PRM}^{\sigma}_d(2)$.

On the other hand, we saw previously that the condition $\bigcup_{c_2 \in \mathfrak{I}_{a_2}, c_2 > d-(q^s-1)} \mathfrak{I}_{(d-c_2,c_2)} \subset \Delta_{\leq d}$ is satisfied in this case. Hence, adding homogenized field equations to $f^r_{a_2}$ as we did to obtain the set B_2, we can obtain a polynomial $g^r_{a_2}$ such that $g^r_{a_2}(1, x_1, x_2) = f^r_{a_2}(1, x_1, x_2)$, $g^r_{a_2}(0, 1, x_1) = \mathcal{T}_{a_2}(\xi^r_{a_2}x_2^{a_2}), g^r_{a_2}(0, 0, 1) = 0$. Note that in this case we are not using the homogenized field equation $x_2^{\overline{d}}(1-x_0)$ to construct $g^r_{a_2}$ since we already have the monomial $x_1^{q^s-1}x_2^{\overline{d}}$ in the support of $f^r_{a_2}$, which reduces to $x_2^{\overline{d}}$ when setting $x_0 = 0, x_1 = 1$. It is easy to check that the polynomial

$$h^r_{a_2} = x_0 \left(\sum_{c \in Y_{a_2}} \mathcal{T}_c(\xi^r_{a_2} x_1^{c_1} x_2^{c_2}) \right) + (1 - x_0)x_1 \mathcal{T}_{a_2}(\xi^r_{a_2} x_2^{a_2}),$$

where ξ_{a_2} is a primitive element in $\mathbb{F}_{q^{n_{a_2}}}$, has the same evaluation in P^2 as $g^r_{a_2}$. Therefore, the evaluation of the polynomials $h^r_{a_2}$ is equivalent modulo $S/I(P^2)$ to the evaluation of some homogeneous polynomials of degree d, and they evaluate to $\mathbb{F}_q$, which means that the evaluation of the polynomials $h^r_{a_2}$ is in $\mathrm{PRM}^{\sigma}_d(2)$. We can now define the set B_3 in the following way:

(a) If $\mathfrak{I}_{(q^s-1,\overline{d})} \subset \Delta_{\leq d}$, we set $B_3 = \{l_{a_2} - x_0 \mathcal{T}_{(q^s-1,a_2)}(x_1^{q^s-1}x_2^{a_2})\} \cup \{h^r_{a_2}, 0 \leq r \leq n_{a_2} - 1\}$.

(b) If $\mathfrak{I}_{(q^s-1,\overline{d})} \not\subset \Delta_{\leq d}$:

  (b.1) If $\bigcup_{c_2 \in \mathfrak{I}_{a_2}, c_2 > d-(q^s-1)} \mathfrak{I}_{(d-c_2,c_2)} \subset \Delta_{\leq d}$, we set $B_3 = \{l_{a_2}\}$.

  (b.2) We set $B_3 = \emptyset$ otherwise.

With this definition, we can summarize everything discussed thus far in the following result.

Lemma C.3.23. *Let $1 \leq d \leq 2(q^s - 1)$ and let $a_2 \in \mathcal{A}^1$ such that $\mathfrak{I}_{a_2} = \mathfrak{I}_{\overline{d}}$. If $B_3 \neq \emptyset$, the evaluation of the set B_3 is in $\mathrm{PRM}^{\sigma}_d(2)$, and the evaluation of the set $B = B_1 \cup B_2 \cup B_3$ is linearly independent.*

Proof. In the previous discussion we have seen that, under the stated conditions, the evaluation of the polynomials in B_3 is in $\mathrm{PRM}_d^\sigma(2)$, i.e., for each polynomial in B_3, a homogeneous polynomial of degree d with the same evaluation can be constructed, and it evaluates to $\mathbb{F}_q$.

The set $B_1 \cup B_2$ is linearly independent due to Lemma C.3.20. The polynomial l_{a_2} (respectively, the polynomial $l_{a_2} - x_0\mathcal{T}_{(q^s-1,a_2)}(x_1^{q^s-1}x_2^{a_2})$) is not contained in the span of $B_1 \cup B_2$ since it is the only polynomial that we are considering with nonzero evaluation at $[0:0:1]$. With this in mind, the same argument as in Lemma C.3.20 proves that the evaluation of the rest of polynomials in B_3 (if any) is linearly independent, and the evaluation of these polynomials is also linearly independent with the evaluation of the polynomials in $B_1 \cup B_2$. □

Remark C.3.24. We can argue as in Remark C.3.21 to construct simpler polynomials than the polynomials $h_{a_2}^r$ and l_{a_2}. This gives rise to a set B_3' with the properties stated in Lemma C.3.23.

Example C.3.25. Let us continue with the setting from C.3.22. We did not study the case $a_2 = 3$ because $\mathfrak{I}_{a_2} = \mathfrak{I}_3 = \mathfrak{I}_{\overline{d}} = \mathfrak{I}_6$. This case is covered by Lemma C.3.23, and we construct the set B_3' from Remark C.3.24 in this example. Following the statement of Lemma C.3.23, we check first if $\mathfrak{I}_{(q^s-1,\overline{d})} \subset \Delta_{\leq d}$, for $d = 21$, $\overline{d} = 6$ and $q^s - 1 = 15$. We have

$$\mathfrak{I}_{(15,6)} = \{(15,3),(15,6),(15,9),(15,12)\}.$$

We see that $\mathfrak{I}_{(15,6)} \not\subset \Delta_{\leq 21}$, for example we have $(15,9)$ with $15+9 = 24 > 21$.

Now we have to verify the condition (C.3.9). The only elements c_2 in $\mathfrak{I}_{a_2} = \{3,6,9,12\}$ such that $c_2 > \overline{d}$ are 9 and 12. The corresponding cyclotomic sets $\mathfrak{I}_{(21-9,9)}$ and $\mathfrak{I}_{(21-12,12)}$ are

$$\mathfrak{I}_{(9,3)} = \{(9,3),(3,6),(12,9),(6,12)\},$$
$$\mathfrak{I}_{(6,3)} = \{(6,3),(12,6),(3,9),(9,12)\}.$$

Hence, we see that the condition (C.3.9) is satisfied since both cyclotomic sets are contained in $\Delta_{\leq 21}$. Therefore, we have to construct l_{a_2}, for which we have to compute Y_3. We have $\mathfrak{I}_{(21-6,6)} = \mathfrak{I}_{(15,3)}$ from before, but we have seen that this cyclotomic set is not contained in $\Delta_{\leq 21}$. Thus, $(15,3) \notin Y_3$. On the other hand, we have just seen that $(6,3),(9,3) \in Y_{a_2}$, as both of them are contained in $\Delta_{\leq 21}$. The last cyclotomic set that we have to consider is the following:

$$\mathfrak{I}_{(\overline{21-3},3)} = \{(3,3),(6,6),(9,9),(12,12)\},$$

which is not contained in $\Delta_{\leq 21}$. Hence, $Y_3 = \{(6,3),(9,3)\}$. Using Remarks C.3.21 and C.3.24 in this case gives $Y_3' = Y_3$, which means that we have $B_3' = B_3$. The only polynomial in B_3 is

$$l_3 = x_0\left(\mathcal{T}_{(9,3)}(x_1^9x_2^3) + \mathcal{T}_{(6,3)}(x_1^6x_2^3)\right) + (1-x_0)x_1\mathcal{T}_3(x_2^3) + (1-x_0)(1-x_1)x_2^{21}.$$

We obtain that there are 133 polynomials in $B_1 \cup B_2 \cup B_3$, with linearly independent evaluation, and this evaluation is in $\mathrm{PRM}_{21}^\sigma(2)$.

The following results show that the case where $1 \leq d \leq q^s - 1$ is particularly simple.

Lemma C.3.26. *Let $1 \leq d \leq q^s - 1$ .We have that $|I_d| = 1$ if and only if $d = \lambda \frac{q^s-1}{q-1}$, for some integer $1 \leq \lambda \leq q-1$.*

Proof. We only need to observe that

$$|I_d| = 1 \iff dq \equiv d \bmod q^s - 1 \iff d(q-1) = \lambda(q^s-1) = \lambda(q-1)\frac{q^s-1}{q-1}$$
$$\iff d = \lambda\frac{q^s-1}{q-1}, \text{ for some } 1 \leq \lambda \leq q-1.$$

□

Proposition C.3.27. *Let $1 \leq d \leq q^s - 1$. Then $B_3 \neq \emptyset$ if and only if d is a multiple of $\frac{q^s-1}{q-1}$. In that situation*

$$B_3 = \{x_2^d\}.$$

Proof. If d is a multiple of $\frac{q^s-1}{q-1}$, by Lemma C.3.26, we have that $|\mathfrak{I}_d| = 1$ and $\mathfrak{I}_{(0,d)} \subset \Delta_{\leq d}$. By Lemma C.3.23, $B_3 = \{l_d\}$. We have $Y_d = \{(0,d)\}$ from its definition. Then, by the definition of l_d we have $l_d = x_0\mathcal{T}_{(0,d)}(x_2^d) + (1-x_0)x_1\mathcal{T}_d(x_2^d) + (1-x_0)(1-x_1)x_2^d = x_0x_2^d + (1-x_0)x_1x_2^d + (1-x_0)(1-x_1)x_2^d = x_2^d$.

On the other hand, if $B_3 \neq \emptyset$ and we consider $a_2 \in \mathcal{A}^1_{\leq d}$ with $\mathfrak{I}_{a_2} = \mathfrak{I}_d$, by Lemma C.3.23 we have that $\bigcup_{c_2 \in \mathfrak{I}_{a_2}} \mathfrak{I}_{(d-c_2,c_2)} \subset \Delta_{\leq d}$. Using Lemma C.3.26, we assume that $|\mathfrak{I}_{a_2}| > 1$, and we will obtain a contradiction. Let $e \in \mathfrak{I}_{a_2}$ with $e \neq d$. This implies that there is an integer $l > 0$ such that $d \equiv q^l e \bmod q^s - 1$. Therefore, we have $(\overline{q^l(d-e)}, d) \in \mathfrak{I}_{(d-e,e)}$, with $\overline{q^l(d-e)} \neq 0$. This implies that $\mathfrak{I}_{(d-e,e)} \not\subset \Delta_{\leq d}$, a contradiction. □

In order to assert that B is a basis, we would need to show that B generates the whole code $\mathrm{PRM}_d^\sigma(2)$. However, we have already computed the dimension for $\mathrm{PRM}_d^{\sigma,\perp}(2)$. By Lemma C.3.23, we know that the evaluation of the polynomials in B is linearly independent, which means that if we show that $|B| = n - \dim \mathrm{PRM}_d^{\sigma,\perp}(2)$, then this implies that B is a basis. To see this, we will introduce a new decomposition of the sets B and D.

Let $1 \leq d \leq 2(q^s-1)$, and $d^\perp = 2(q^s-1) - d$. For the set B, we first define $\Gamma_1 = B_1$. On the other hand, let $a_2 \in \mathcal{A}^1$ such that $\mathfrak{I}_{a_2} = \mathfrak{I}_{\overline{d}}$, and we define Γ_2 in the following way:

1. If $\mathfrak{I}_{(q^s-1,\overline{d})} \subset \Delta_{\leq d}$, we set

$$\Gamma_2 = B_2 \cup \{h_{a_2}^r, 0 \leq r \leq n_{a_2} - 1\}.$$

2. We set

$$\Gamma_2 = B_2,$$

otherwise.

And we define $\Gamma_3 = B \setminus (\Gamma_1 \cup \Gamma_2)$. Equivalently, we consider the following definition:

(a) If $\mathfrak{I}_{(q^s-1,\overline{d})} \subset \Delta_{\leq d}$, we set

$$\Gamma_3 = \{l_{a_2} - x_0\mathcal{T}_{(q^s-1,a_2)}(x_1^{q^s-1}x_2^{a_2})\}.$$

(b) If $\mathfrak{I}_{(q^s-1,\overline{d})} \not\subset \Delta_{\leq d}$:

(b.1) If $\bigcup_{c_2 \in \mathfrak{I}_{a_2}, c_2 > d-(q^s-1)} \mathfrak{I}_{(d-c_2,c_2)} \subset \Delta_{\leq d}$, we set

$$\Gamma_3 = \{l_{a_2}\}.$$

(b.2) We set

$$\Gamma_3 = \emptyset,$$

otherwise.

It is clear by construction that $B = \Gamma_1 \cup \Gamma_2 \cup \Gamma_3$. The idea behind this decomposition is that in Γ_1 we have sets of size n_a for some $a \in \mathcal{A}$, in Γ_2 we have sets of size n_{a_2} for some $a_2 \in \mathcal{A}^1$, and in Γ_3 we have a set of size 1 (if any). Now we define a similar decomposition for D, and we will see later why we are interested in this decomposition.

For the set D, we define first $\Gamma_1^\perp = D_1$. Let $a_2 \in \mathcal{A}^1$ such that $\mathfrak{I}_{a_2} = \mathfrak{I}_{\overline{d}}$. Now we define $\Gamma_3^\perp$ as follows:

1. If there is an element $c \in \mathcal{A}$ such that $c_2 = a_2$, $\mathfrak{I}_c \neq \mathfrak{I}_{(0,\overline{d^\perp})}$, and $M_c(d^\perp)$ contains monomials of the two types, we set

$$\Gamma_3^\perp = (x_0 - 1)(x_1 - 1).$$

2. We set

$$\Gamma_3^\perp = \emptyset,$$

otherwise.

We can now define $\Gamma_2^\perp = D \setminus (\Gamma_1^\perp \cup \Gamma_3^\perp)$. This can also be expressed in the following way:

$$\Gamma_2^\perp = (D_2 \cup D_3 \cup D_4) \setminus \{(x_0 - 1)(x_1 - 1)\}. \tag{C.3.10}$$

Again, by construction we have $D = \Gamma_1^\perp \cup \Gamma_2^\perp \cup \Gamma_3^\perp$.

Remark C.3.28. The condition in (1) from the definition of $\Gamma_3^\perp$ implies that $M_{(0,\overline{d^\perp})}(d^\perp)$ contains monomials of the two types. Indeed, if $d^\perp \geq q^s$, $M_{(0,\overline{d^\perp})}(d^\perp)$ always contains monomials of the two types, and if $d^\perp \leq q^s - 1$ and there is an element $c \in \mathcal{A}$ such that $c_2 = a_2$, $\mathfrak{I}_c \neq \mathfrak{I}_{(0,\overline{d^\perp})}$, and $M_c(d^\perp)$ contains monomials of the two types, this means that there is $\gamma \in \mathfrak{I}_c$ with $\gamma_1 > 0$ such that $\gamma_1 + \gamma_2 = d^\perp$ by Lemma C.3.7, with $\gamma_2 \in \mathfrak{I}_{d^\perp}$. Therefore, $d^\perp$ is not the minimal element in $\mathfrak{I}_{d^\perp}$, which means that $M_{(0,d^\perp)}(d^\perp)$ contains monomials of the two types. Hence, we have $(x_0 - 1)(x_1 - 1) \in \Gamma_3^\perp$ if and only if $(x_0 - 1)(x_1 - 1) \in D_3$.

Let $b_2 \in \mathcal{A}^1$ such that $\mathfrak{I}_{b_2} = \mathfrak{I}_{\overline{d}}$, for some degree $1 \leq d \leq 2(q^s - 1)$. For ease of use, we recall here the sizes of the set we have just defined:

(a.1) $|\Gamma_1| = |B_1| = \sum_{a \in \mathcal{A}_{<d}} n_a$.

(a.2) $|\Gamma_2| = |B_2| + n_{\overline{d}} = \sum_{a_2 \in Y} n_{a_2} + n_{\overline{d}}$ if $\mathfrak{I}_{(q^s-1,\overline{d})} \subset \Delta_{\leq d}$, and $|\Gamma_2| = |B_2|$ otherwise.

(a.3) $|\Gamma_3| = 1$ if $\bigcup_{c_2 \in \mathfrak{I}_{b_2}, c_2 > d-(q^s-1)} \mathfrak{I}_{(d-c_2,c_2)} \subset \Delta_{\leq d}$, and $|\Gamma_3| = 0$ otherwise.

(b.1) $\left|\Gamma_1^\perp\right| = |D_1| = \sum_{a\in U} n_a$.

(b.2) $\left|\Gamma_2^\perp\right| = |D_2|+|D_3 \setminus \{(x_0-1)(x_1-1)\}|+|D_4| = \sum_{a_2\in V} n_{a_2}+n_{\overline{d}}+|D_4|$ if $M_{(0,\overline{d^\perp})}(d^\perp)$ contains monomials of the two types, and $\left|\Gamma_2^\perp\right| = \sum_{a_2\in V} n_{a_2}+|D_4|$ otherwise, where $|D_4| = 1$ if $d = q^s-1$, and $|D_4| = 0$ otherwise.

(b.3) $\left|\Gamma_3^\perp\right| = 1$ if there is an element $c \in \mathcal{A}$ such that $c_2 = b_2$, $\mathfrak{I}_c \neq \mathfrak{I}_{(0,\overline{d^\perp})}$, and $M_c(d^\perp)$ contains monomials of the two types, and $\left|\Gamma_3^\perp\right| = 0$ otherwise.

Definition C.3.29. Let $b = (b_1, b_2) \in \mathbb{Z}_{q^s}^2$. We define

$$b' = (b_1', b_2') := (q^s-1-b_1, q^s-1-b_2).$$

Remark C.3.30. Let $c \in \mathcal{A}$. Then $c_2 \in \mathfrak{I}_{a_2}$ if and only if $c_2' = q^s-1-c_2 \in \mathfrak{I}_{a_2'}$.

We are interested in doing these decompositions because the length of these codes is $n = \frac{q^{3s}-1}{q^s-1} = q^{2s}+q^s+1$, and we also have $\sum_{a\in\mathcal{A}} n_a = q^{2s}$, $\sum_{a_2\in\mathcal{A}^1} n_{a_2} = q^s$. We prove now that $|\Gamma_1| + \left|\Gamma_1^\perp\right| = q^{2s}$, $|\Gamma_2| + \left|\Gamma_2^\perp\right| = q^s$ and $|\Gamma_3| + \left|\Gamma_3^\perp\right| = 1$. This is reminiscent of the affine case, in which if we evaluate the traces corresponding to $a \in \mathcal{A}$ for the primary code, then for the dual code we do not need to consider the traces corresponding to $\mathfrak{I}_{a'}$. The strategy in our case will be similar: for each $a \in \mathcal{A}$ such that we consider its traces in B, we will see that we do not consider the traces corresponding to $\mathfrak{I}_{a'}$ in D. We start with the sets Γ_1 and $\Gamma_1^\perp$.

Lemma C.3.31. *With the definitions as above, we have* $|\Gamma_1| + \left|\Gamma_1^\perp\right| = q^2$.

Proof. By definition, it is clear that we have $q^{2s} - |\Gamma_1| = \sum_{a\in\mathcal{A}\setminus\mathcal{A}_{<d}} n_a$. We note that $a \in \mathcal{A}\setminus\mathcal{A}_{<d}$ if and only if there is $(c_1,c_2) \in \mathfrak{I}_a$ such that $c_1+c_2 \geq d$. Therefore, $2(q^s-1)-c_1-c_2 = c_1'+c_2' \leq d^\perp$, which means that $M_{a'}(d^\perp) \neq \emptyset$. It is easy to see that $n_a = n_{a'}$, and we have $\sum_{a\in\mathcal{A}\setminus\mathcal{A}_{<d}} n_a = \sum_{a'\in\mathcal{A}|M_{a'}(d^\perp)\neq\emptyset} n_{a'} = \left|\Gamma_1^\perp\right|$. Thus, $|\Gamma_1| + \left|\Gamma_1^\perp\right| = q^{2s}$. □

For the case of Γ_2 and $\Gamma_2^\perp$, we need the following technical results.

Lemma C.3.32. *Let* $1 \leq d \leq 2(q^s-1)$, $d^\perp = 2(q^s-1)-d$ *and* $c \in \mathcal{A}$. *Then* $M_{c'}(d^\perp)$ *contains monomials of the two types if and only if* $\mathfrak{I}_c \cap (\Delta_d \cup \Delta_{2(q^s-1)-\overline{d^\perp}}) \neq \emptyset$ *and* $\mathfrak{I}_c \not\subset \Delta_{\leq d}$, *where* $\Delta_z = \emptyset$ *if* $z < 0$.

Proof. By Lemma C.3.7, $M_{c'}(d^\perp)$ contains monomials of the two types if and only if $\mathfrak{I}_{c'} \cap \Delta_{<d^\perp} \neq \emptyset$ and $\mathfrak{I}_{c'} \cap (\Delta_{d^\perp} \cup \Delta_{\overline{d^\perp}}) \neq \emptyset$. The condition $\mathfrak{I}_{c'} \cap \Delta_{<d^\perp} \neq \emptyset$ implies that there is $(\gamma_1',\gamma_2') \in \mathfrak{I}_{c'}$ such that $2(q^s-1)-\gamma_1-\gamma_2 < d^\perp \iff \gamma_1+\gamma_2 > d$. Thus, $\gamma \in \mathfrak{I}_c \not\subset \Delta_{\leq d}$. The condition $\mathfrak{I}_{c'} \cap (\Delta_{d^\perp} \cup \Delta_{\overline{d^\perp}}) \neq \emptyset$ implies that there is an element $(\gamma_1',\gamma_2') \in \mathfrak{I}_{c'}$ with either $2(q^s-1)-\gamma_1-\gamma_2 = d^\perp$ or $2(q^s-1)-\gamma_1-\gamma_2 = \overline{d^\perp}$. Hence, $\gamma \in \Delta_d \cup \Delta_{2(q^s-1)-\overline{d^\perp}}$. □

Remark C.3.33. It is easy to check that $2(q^s-1)-\overline{d^\perp} = d$ if $d \geq q^s-1$, and $2(q^s-1)-\overline{d^\perp} = d+q^s-1$ if $d \leq q^s-2$.

The following result, among other things, relates the set

$$Y = \left\{ a_2 \in \mathcal{A}^1_{\leq d}, \mathfrak{I}_{a_2} \neq \mathfrak{I}_{\overline{d}} \mid \bigcup_{c_2 \in \mathfrak{I}_{a_2}, c_2 > d-(q^s-1)} \mathfrak{I}_{(d-c_2,c_2)} \subset \Delta_{\leq d} \right\} \tag{C.3.11}$$

with the set $V = \{a_2 \in \mathcal{A}^1 \mid \mathfrak{I}_{a_2} \neq \mathfrak{I}_{\overline{d^\perp}}$ and $\exists\ c \in \mathcal{A}$ with $c_2 = a_2$ and $M_c(d^\perp)$ contains monomials of the two types$\}$.

Lemma C.3.34. *Let $a_2 \in \mathcal{A}^1_{\leq d}$. Then $\bigcup_{c_2 \in \mathfrak{I}_{a_2}, c_2 > d-(q^s-1)} \mathfrak{I}_{(d-c_2,c_2)} \subset \Delta_{\leq d}$ if and only if there is no $c \in \mathcal{A}$ with $\mathfrak{I}_{c'} \neq \mathfrak{I}_{(0,\overline{d^\perp})}$, $c_2' \in \mathfrak{I}_{a_2'}$, and such that $M_{c'}(d^\perp)$ contains monomials of the two types.*

Proof. Let $a_2 \in \mathcal{A}^1_{\leq d}$. By Lemma C.3.32, we can translate the statement to the following: we have $\bigcup_{c_2 \in \mathfrak{I}_{a_2}, c_2 > d-(q^s-1)} \mathfrak{I}_{(d-c_2,c_2)} \subset \Delta_{\leq d}$ if and only if there is no $c \in \mathcal{A}$, $\mathfrak{I}_c \neq \mathfrak{I}_{(q^s-1,\overline{d^\perp}')}$, with $c_2 = a_2$, $\mathfrak{I}_c \cap (\Delta_d \cup \Delta_{2(q^s-1)-\overline{d^\perp}}) \neq \emptyset$ and $\mathfrak{I}_c \not\subset \Delta_{\leq d}$. In what follows, we will use this last statement instead of the original one. We also note that $\overline{d^\perp}' = \overline{d}$ if $d \neq q^s-1$, and $\overline{d^\perp}' = 0$ if $d = q^s-1$.

We assume that $\bigcup_{c_2 \in \mathfrak{I}_{a_2}, c_2 > d-(q^s-1)} \mathfrak{I}_{(d-c_2,c_2)} \subset \Delta_{\leq d}$ and we consider $c \in \mathcal{A}$, $\mathfrak{I}_c \neq \mathfrak{I}_{(q^s-1,\overline{d^\perp}')}$, with $c_2 = a_2$. If $\mathfrak{I}_c \cap \Delta_d \neq \emptyset$, we have $(d-\gamma_2, \gamma_2) \in \mathfrak{I}_c$ for some $\gamma_2 \in \mathfrak{I}_{a_2}$. This implies that $d - \gamma_2 \leq q^s - 1$, i.e., $\gamma_2 \geq d - (q^s-1)$. If $\gamma_2 > d-(q^s-1)$, then, by our assumptions, $\mathfrak{I}_c = \mathfrak{I}_{(d-\gamma_2,\gamma_2)} \subset \Delta_{\leq d}$. If we had $\gamma_2 = d-(q^s-1)$ and $d \geq q^s$, then this would imply that $(q^s-1, \overline{d}) \in \mathfrak{I}_c$, which is a contradiction with the fact that $\mathfrak{I}_c \neq \mathfrak{I}_{(q^s-1,\overline{d})}$. If $d = q^s-1$, then $\gamma_2 = 0$, which implies that $(d-\gamma_2, \gamma_2) = (q^s-1, 0)$ and $\mathfrak{I}_c = \{(q^s-1, 0)\}$, a contradiction with the fact that $\mathfrak{I}_c \neq \mathfrak{I}_{(q^s-1,\overline{d^\perp}')} = \mathfrak{I}_{(q^s-1,0)}$.

On the other hand, if $\mathfrak{I}_c \cap \Delta_d = \emptyset$ and $\mathfrak{I}_c \cap \Delta_{2(q^s-1)-\overline{d^\perp}} \neq \emptyset$, we have $\gamma \in \mathfrak{I}_c$ with $\gamma_1 + \gamma_2 = 2(q^s-1) - \overline{d^\perp}$, and $\gamma_2 \in \mathfrak{I}_{a_2}$. Considering Remark C.3.33, if $d \geq q^s-1$, this implies $\gamma \in \Delta_d$, a contradiction with the assumption $\mathfrak{I}_c \cap \Delta_d = \emptyset$. If $d \leq q^s-2$, then we note that $\gamma_2 \leq d$ since $a_2 \in \mathcal{A}_{\leq d}$, and $\gamma_1 \leq q^s-1$, which implies $\gamma_1 + \gamma_2 \leq d + q^s - 1 = 2(q^s-1) - \overline{d^\perp}$. We can only obtain the equality if $\gamma_1 = q^s-1$ and $\gamma_2 = d$, which is a contradiction with the assumption $\mathfrak{I}_c \neq \mathfrak{I}_{(q^s-1,\overline{d})}$.

For the other implication, we assume now that there is no $c \in \mathcal{A}$, $\mathfrak{I}_c \neq \mathfrak{I}_{(q^s-1,\overline{d^\perp}')}$, with $c_2 = a_2$, $\mathfrak{I}_c \cap (\Delta_d \cup \Delta_{2(q^s-1)-\overline{d^\perp}}) \neq \emptyset$ and $\mathfrak{I}_c \not\subset \Delta_{\leq d}$. For each $\gamma_2 \in \mathfrak{I}_{a_2}$, with $\gamma_2 > d-(q^s-1)$, there is an element $c \in \mathcal{A}$ such that $\mathfrak{I}_c = \mathfrak{I}_{(d-\gamma_2,\gamma_2)}$. Because of the ordering chosen for the elements in $\mathbb{Z}_{q^s}^2$, we must have $c_2 = a_2$. We clearly have $(d-\gamma_2, \gamma_2) \in \mathfrak{I}_c \cap \Delta_d \neq \emptyset$. By our assumption, we must have $\mathfrak{I}_c = \mathfrak{I}_{(d-\gamma_2,\gamma_2)} \subset \Delta_{\leq d}$. □

Remark C.3.35. Lemma C.3.34 implies the following. Let $a_2 \in \mathcal{A}^1_{\leq d}$ with $\mathfrak{I}_{a_2} \neq \mathfrak{I}_{\overline{d}}$. Then $a_2 \in Y$ if and only if there is no $c \in \mathcal{A}$ with $c_2' \in \mathfrak{I}_{a_2'}$, $\mathfrak{I}_{c'} \neq \mathfrak{I}_{(0,\overline{d^\perp})}$, and such that $M_{c'}(d^\perp)$ contains monomials of the two types.

Recalling that $\overline{d}' = \overline{d^\perp}$ if $d \neq q^s-1$, and $\overline{d}' = 0$ if $d = q^s-1$, we see that if $d \neq q^s-1$, $\mathfrak{I}_{a_2} \neq \mathfrak{I}_{\overline{d}}$ together with $c_2' \in \mathfrak{I}_{a_2'}$ already implies $\mathfrak{I}_{c'} \neq \mathfrak{I}_{(0,\overline{d^\perp})}$. For $d = q^s-1$, in the case $a_2 = 0$, we see that the previous statement says: $0 \in Y$ if and only if there is no $c \in \mathcal{A}$ with $c_2' \in \mathfrak{I}_{q^s-1}$, $\mathfrak{I}_{c'} \neq \mathfrak{I}_{(0,q^s-1)}$, and such that $M_{c'}(q^s-1)$ contains monomials of the two

types. However, $M_{(0,q^s-1)}(q^s-1) = \{x_2^{q^s-1}\}$ does not have monomials of the two types. Therefore, in this case we can also omit the condition $\mathfrak{I}_{c'} \neq \mathfrak{I}_{(0,\overline{d^\perp})}$.

Thus, we have the following statement. Let $a_2 \in \mathcal{A}^1_{\leq d}$ with $\mathfrak{I}_{a_2} \neq \mathfrak{I}_{\overline{d}}$. Then $a_2 \in Y$ if and only if there is no $c \in \mathcal{A}$ with $c'_2 \in \mathfrak{I}_{a'_2}$ and such that $M_{c'}(d^\perp)$ contains monomials of the two types.

Lemma C.3.36. *Let $1 \leq d \leq 2(q^s-1)$, $d^\perp = 2(q^s-1)-d$. If $d \neq q^s-1$, then $M_{(0,\overline{d^\perp})}(d^\perp)$ contains monomials of the two types if and only if $\mathfrak{I}_{(q^s-1,\overline{d})} \not\subset \Delta_{\leq d}$.*

Proof. If $d^\perp \geq q^s$, then $M_{(0,\overline{d^\perp})}(d^\perp)$ contains monomials of the two types because $x_0^{q^s-1}x_2^{\overline{d^\perp}}$, $x_2^d \in M_{(0,\overline{d^\perp})}(d^\perp)$. In this case, we have $d \leq q^s-2$, which ensures that $\mathfrak{I}_{(q^s-1,\overline{d})} \not\subset \Delta_{\leq d}$.

If $d^\perp \leq q^s-1$, $M_{(0,d^\perp)}(d^\perp)$ contains monomials of the two types if and only if $d^\perp$ is not the minimal element of $\mathfrak{I}_{d^\perp}$. We have $(d^\perp)' = q^s-1-d^\perp = q^s-1-(2(q^s-1)-d) = d-(q^s-1)$. The condition $d^\perp \leq q^s-1$ implies that $d \geq q^s-1$. Taking into account the assumption $d \neq q^s-1$, we can assume now that $d > q^s-1$. Thus, $(d^\perp)' = \overline{d}$, and we obtain that $M_{(0,d^\perp)}(d^\perp)$ contains monomials of the two types if and only if $d^\perp$ is not the minimal element of $\mathfrak{I}_{d^\perp}$, which happens if and only if $(d^\perp)' = \overline{d}$ is not the maximal element of $\mathfrak{I}_{\overline{d}}$, which happens if and only if $\mathfrak{I}_{(q^s-1,\overline{d})} \not\subset \Delta_{\leq d}$. □

Lemma C.3.37. *We have that $|\Gamma_2| + \left|\Gamma_2^\perp\right| = q^s$.*

Proof. We start with the following decomposition:

$$q^s = \sum_{a_2 \in \mathcal{A}^1} n_{a_2} = \sum_{a_2 \in \mathcal{A}^1_{\leq d}, a_2 \in Y, \mathfrak{I}_{a_2} \neq \mathfrak{I}_{\overline{d}}} n_{a_2} + \sum_{a_2 \in \mathcal{A}^1_{\leq d}, a_2 \notin Y, \mathfrak{I}_{a_2} \neq \mathfrak{I}_{\overline{d}}} n_{a_2} + \sum_{a_2 \in \mathcal{A}^1 \setminus \mathcal{A}^1_{\leq d}, \mathfrak{I}_{a_2} \neq \mathfrak{I}_{\overline{d}}} n_{a_2} + n_{\overline{d}}.$$

We recall that $\sum_{a_2 \in \mathcal{A}^1_{\leq d}, a_2 \in Y, \mathfrak{I}_{a_2} \neq \mathfrak{I}_{\overline{d}}} n_{a_2} = |B_2|$. We also recall the definition $V = \{a_2 \in \mathcal{A}^1 \mid \mathfrak{I}_{a_2} \neq \mathfrak{I}_{\overline{d^\perp}}$ and $\exists\, c \in \mathcal{A} \mid c_2 = a_2$ and $M_c(d^\perp)$ contains monomials of the two types$\}$. Let $a_2 \in \mathcal{A}^1_{\leq d}$. By Remark C.3.35, if $d \neq q^s-1$, we have that $a_2 \in Y$ if and only if the minimal element of $\mathfrak{I}_{a'_2}$ is not in V. Taking into account that $n_{a_2} = n_{a'_2}$, we have that

$$\sum_{a_2 \in \mathcal{A}^1_{\leq d}, a_2 \notin Y, \mathfrak{I}_{a_2} \neq \mathfrak{I}_{\overline{d}}} n_{a_2} = \sum_{b'_2 \in V \mid \mathfrak{I}_{b_2} = \mathfrak{I}_{a_2}, a_2 \in \mathcal{A}^1_{\leq d}} n_{b'_2}.$$

If $d \geq q^s-1$, we have $\mathcal{A}^1_{\leq d} = \mathcal{A}^1$, and the only thing left to do is to consider the cyclotomic set $\mathfrak{I}_{\overline{d}}$. However, if $d \leq q^s-2$, we can consider $a_2 \in \mathcal{A}^1 \setminus \mathcal{A}^1_{\leq d}$. We have that $d \leq q^s-2 \iff d^\perp \geq q^s$, and $a_2 \in \mathcal{A}^1 \setminus \mathcal{A}^1_{\leq d}$ implies that there is $\gamma_2 \in \mathfrak{I}_{a_2}$ with $\gamma_2 > d \iff \gamma'_2 < \overline{d^\perp}$ in this case. Hence, we can consider $c = (\overline{d^\perp} - \gamma'_2, \gamma'_2)$, and we have that $\{x_0^{q^s-1}x_1^{\overline{d^\perp}-\gamma'_2}x_2^{\gamma'_2}, x_1^{d^\perp-\gamma'_2}x_2^{\gamma'_2}\} \subset M_c(d^\perp)$, which means that $M_c(d^\perp)$ contains monomials of the two types, and $\mathfrak{I}_{a'_2} \neq \mathfrak{I}_{\overline{d^\perp}}$, i.e., if we consider $b_2 \in \mathcal{A}^1$ such that $\mathfrak{I}_{b_2} = \mathfrak{I}_{a'_2}$, we have $b_2 \in V$.

Reciprocally, if we consider $a_2 \in \mathcal{A}^1$ and we have $c' \in \mathcal{A}$ such that $c'_2 \in \mathfrak{I}_{a'_2} \neq \mathfrak{I}_{\overline{d^\perp}}$ and $M_{c'}(d^\perp)$ contains monomials of the two types, there is $(\gamma'_1, \gamma'_2) \in \mathfrak{I}_c$ with $\gamma'_1 + \gamma'_2 = \overline{d^\perp} = d^\perp - (q^s-1)$, which means that $\gamma_1 + \gamma_2 = d + (q^s-1)$, with $\gamma_2 \in \mathfrak{I}_{a_2}$. If $\gamma_1 < q^s-1$, then

$\gamma_2 > d$ and $a_2 \in \mathcal{A} \setminus \mathcal{A}_{\leq d}$. If $\gamma_1 = q^s - 1$, then $\gamma_2 = d$, a contradiction since in this case $\mathfrak{I}_{a_2'} \neq \mathfrak{I}_{\overline{d^\perp}}$ implies $\mathfrak{I}_{a_2} \neq \mathfrak{I}_d$.

Thus, we have obtained that

$$\sum_{a_2 \in \mathcal{A}^1_{\leq d}, a_2 \notin Y, \mathfrak{I}_{a_2} \neq \mathfrak{I}_{\overline{d}}} n_{a_2} + \sum_{a_2 \in \mathcal{A}^1 \setminus \mathcal{A}^1_{\leq d}, \mathfrak{I}_{a_2} \neq \mathfrak{I}_{\overline{d}}} n_{a_2} = \sum_{b_2' \in V} n_{b_2'} = |D_2|.$$

We now focus on the cyclotomic set $\mathfrak{I}_{\overline{d}}$. We use Lemma C.3.36, as we are still in the case $d \neq q^s - 1$. If $d < q^s - 1$, we always have $|\Gamma_2| = |B_2|$ by definition, and we also have $|\Gamma_3| = |D_2| + n_d$ because $\{x_0^{q^s-1} x_2^{\overline{d^\perp}}, x_2^{d^\perp}\} \subset M_{(0,\overline{d^\perp})}(d^\perp)$, i.e., $M_{(0,\overline{d^\perp})}(d^\perp)$ contains monomials of the two types. If $d > q^s - 1$, we have $|\Gamma_2| = |B_2| + n_{\overline{d}}$ if and only if $M_{(0,d^\perp)}(d^\perp)$ does not have monomials of the two types, by Lemma C.3.36, and $|\Gamma_2| = |B_2|$ otherwise. Thus, we have that $|\Gamma_2| = |B_2| + n_{\overline{d}}$ if and only if $\left|\Gamma_2^\perp\right| = |D_2|$, and $|\Gamma_2| = |B_2|$ if and only if $\left|\Gamma_2^\perp\right| = |D_2| + n_{\overline{d}}$. Hence, for $d \neq q^s - 1$ we have proved that

$$|\Gamma_2| + \left|\Gamma_2^\perp\right| = q^s.$$

On the other hand, if $d = q^s - 1$, the condition $\mathfrak{I}_{a_2} \neq \mathfrak{I}_{\overline{d}} = \mathfrak{I}_{q^s-1}$ implies $\mathfrak{I}_{a_2'} \neq \mathfrak{I}_0$ instead of $\mathfrak{I}_{a_2'} \neq \mathfrak{I}_{\overline{d^\perp}} = \mathfrak{I}_{q^s-1}$. For any $a_2 \in \mathcal{A}^1_{\leq d} = \mathcal{A}^1$, $a_2 \notin \{0, q^s - 1\}$, the previous relations between elements in Y and elements in V hold by Remark C.3.35. For $a_2 = 0$ and $a_2 = q^s - 1$ we have that $M_{(0,q^s-1)}(q^s - 1)$ and $M_{(q^s-1,0)}(q^s - 1)$ are the only sets $M_c(d^\perp)$ with $c_2 = 0'$ or $c_2 = (q^s - 1)'$, respectively, such that x_0 does not divide all the monomials in $M_c(q^s - 1)$, and none of them contains monomials of the two types. Hence, for $d = q^s - 1$, we obtain that $0 \notin V$, and also that $|D_2| = \sum_{a_2' \in V} n_{a_2'}$ since $M_{(0,q^s-1)}(q^s - 1)$ does not have monomials of the two types, and there is no other $c \in \mathcal{A}$ with $c_2 = q^s - 1$ such that $M_c(q^s - 1)$ contains monomials of the two types. On the other hand, for $d = q^s - 1$ is easy to see that $0 \in Y$. Moreover, for $d = q^s - 1$ we have that $\mathcal{A}^1 \setminus \mathcal{A}^1_{\leq d} = \emptyset$, and we have $\mathfrak{I}_{(q^s-1,q^s-1)} \not\subset \Delta_{q^s-1}$, which means that $|\Gamma_2| = |B_2| = \sum_{a_2 \in Y} n_{a_2}$. Summarizing all of this, we have

$$|\Gamma_2| + |D_2| + n_{q^s-1} = q^s,$$

because for any $a_2 \in \mathcal{A}^1$, $a_2 \notin \{0, q^s - 1\}$, we have that either $a_2 \in Y$ or $a_2' \in V$ as before, and we have that $0 \in Y$, $q^s - 1 \notin Y$ and $q^s - 1 \notin V$. Obviously, in this case $n_{q^s-1} = 1$, and for $d = q^s - 1$, looking at the definition of $\Gamma_2^\perp$ from (C.3.10), we see that $\left|\Gamma_2^\perp\right| = |D_2| + 1$ (the previous argument shows that, in this case $D_3 = \emptyset$). Therefore, $|\Gamma_2| + \left|\Gamma_2^\perp\right| = q^s$. □

Lemma C.3.38. *We have that* $|\Gamma_3| + \left|\Gamma_3^\perp\right| = 1$.

Proof. Let $a_2 \in \mathcal{A}^1$ such that $\mathfrak{I}_{a_2} = \mathfrak{I}_{\overline{d^\perp}}$. By Remark C.3.28, we have that $\Gamma_3^\perp \neq \emptyset$ if and only if there is an element $c \in \mathcal{A}$ such that $c_2 = a_2$, $\mathfrak{I}_c \neq \mathfrak{I}_{(0,\overline{d^\perp})}$, and $M_c(d^\perp)$ contains monomials of the two types. By Lemma C.3.34, this happens if and only if $\bigcup_{c_2 \in \mathfrak{I}_{a_2}, c_2 > d-(q^s-1)} \mathfrak{I}_{(d-c_2,c_2)} \not\subset \Delta_{\leq d}$. By the definition of Γ_3, this happens if and only if $\Gamma_3 = \emptyset$. The cardinality of these sets is 1 if they are nonempty, which implies that $|\Gamma_3| + \left|\Gamma_3^\perp\right| = 1$. □

Now we state the main result of this section.

Theorem C.3.39. *Let $1 \leq d \leq 2(q^s-1)$. The image by the evaluation map of the set*

$$B = B_1 \cup B_2 \cup B_3,$$

with B_1, B_2, B_3 as defined in Lemmas C.3.15, C.3.20 and C.3.23, respectively, forms a basis for the code $\mathrm{PRM}_d^\sigma(2)$.

Proof. By Lemma C.3.23, we know that the image by the evaluation map of the set B is in $\mathrm{PRM}_d^\sigma(2)$, and it is linearly independent. By Lemmas C.3.31, C.3.37 and C.3.38, we have that $|B| + |D| = |B| + \dim \mathrm{PRM}_d^{\sigma,\perp}(2) = q^2+q+1 = n$. Thus, B is a maximal linearly independent set, and we obtain the result. □

Remark C.3.40. The sets B_2' and B_3' obtained using Remarks C.3.21 and C.3.24, respectively, also satisfy that $B_1 \cup B_2' \cup B_3'$ is a basis for $\mathrm{PRM}_d^\sigma(2)$.

We have that $\mathrm{PRM}_d^\sigma(2)$ is a subcode of $\mathrm{PRM}_d(2)$. Thus, we should be able to obtain $\mathrm{PRM}_d^\sigma(2)$ as the evaluation of some set of homogeneous polynomials of degree d. In fact, in all the discussions leading to Lemmas C.3.15, C.3.20 and C.3.23, we showed how to construct homogeneous polynomials with the same evaluation as the ones considered in Theorem C.3.39. Concrete expressions for these homogeneous polynomials can be given, but they get considerably more involved than the expressions obtained for the polynomials in B.

Example C.3.41. Continuing with Example C.3.25, Theorem C.3.39 states that the image by the evaluation map of the set $B = B_1 \cup B_2' \cup B_3$ that we have constructed in those examples gives a basis for the code $\mathrm{PRM}_{21}^\sigma(2)$. Indeed, it can be checked with Magma [2] that the dimension of $\mathrm{PRM}_{21}^\sigma(2)$ is precisely 133 (the cardinality of B), and that the evaluation of the polynomials in B is in $\mathrm{PRM}_{21}^\sigma(2)$.

Corollary C.3.42. *Let $1 \leq d \leq 2(q^s-1)$. We have the following formula for the dimension of $\mathrm{PRM}_d^\sigma(2)$:*

$$\dim(\mathrm{PRM}_d^\sigma(2)) = |B_1| + |B_2| + |B_3| = \sum_{a \in \mathcal{A}_{<d}} n_a + \sum_{a_2 \in Y} n_{a_2} + \epsilon,$$

where, if we consider $b_2 \in \mathcal{A}^1$ with $\mathfrak{I}_{b_2} = \mathfrak{I}_{\overline{d}}$, then $\epsilon = n_{\overline{d}} + 1$ if $\mathfrak{I}_{(q^s-1,\overline{d})} \subset \Delta_{\leq d}$; $\epsilon = 1$ if $\mathfrak{I}_{(q^s-1,\overline{d})} \not\subset \Delta_{\leq d}$ and $\bigcup_{c_2 \in \mathfrak{I}_{b_2}, c_2 > d-(q^s-1)} \mathfrak{I}_{(d-c_2,c_2)} \subset \Delta_{\leq d}$; and $\epsilon = 0$ otherwise.

We have seen in Lemma C.3.38 that we have the evaluation of a polynomial with x_2^d in its support in $\mathrm{PRM}_d^\sigma(2)$ if and only if we do not have the evaluation of $(x_0-1)(x_1-1)$ in $\mathrm{PRM}_d^{\sigma,\perp}(2)$. If we have the evaluation of $(x_0-1)(x_1-1)$ in $\mathrm{PRM}_d^{\sigma,\perp}(2)$, this implies that $\mathrm{PRM}_d^\sigma(2)$ is a degenerate code, with a common zero at the coordinate associated to $[0:0:1]$ for all its vectors. However, if we only have one common zero, the code that we obtain after puncturing are still different than the ones obtained in the affine case. Nevertheless, if we obtain that all the points in $[\{0\} \times \{1\} \times \mathbb{F}_{q^s}]$ are common zeroes of the vectors in $\mathrm{PRM}_d^\sigma(2)$, then, after puncturing, we obtain a subfield subcode of an affine Reed-Muller code.

The only parameter left to estimate is the minimum distance. For a code C we denote its minimum distance by $\mathrm{wt}(C)$. For the code $\mathrm{PRM}_d^\sigma(2)$ we have the bound given by the minimum distance of $\mathrm{PRM}_d(2)$ (see [20]):

$$\mathrm{wt}(\mathrm{PRM}_d^\sigma(2)) \geq (q^s - t)q^{s(1-r)}, \tag{C.3.12}$$

where $d-1 = r(q^s-1)+t$, $0 \leq t < q^s - 1$. This is the usual way to bound the minimum distance of a subfield subcode, for instance see [12] for the subfield subcodes of projective Reed-Solomon codes. For the subfield subcodes of projective Reed-Muller codes, this bound is sharp in most of the cases that we have checked with Magma [2] ($q^s \leq 9$). For example, in Table C.2 from Section C.5, the bound is sharp except for $d = 2$, which corresponds to a degenerate code, and for $d = 10$ (the bound is 8 instead of 9).

For the dual code $\mathrm{PRM}_d^{\sigma,\perp}(2)$, there is no straightforward bound for the minimum distance, as we see next. Given $C \subset \mathbb{F}_{q^s}^n$, if $C^q = C$, where we understand this as the component wise power of the code, we say that C is Galois invariant. By [1, Thm. 4], we have that $\mathrm{Tr}(C) = C^\sigma$. Writing Theorem C.2.7 as $C^\perp \cap \mathbb{F}_q^n = \mathrm{Tr}(C)^\perp$, we note that $C^{\perp,\sigma} = C^\perp \cap \mathbb{F}_q^n = (C^\sigma)^\perp = C^{\sigma,\perp}$. Therefore, when C is Galois invariant, we have

$$\mathrm{wt}(C^{\sigma,\perp}) = \mathrm{wt}(C^{\perp,\sigma}) \geq \mathrm{wt}(C^\perp).$$

This bound has been used frequently in the affine case [8, 10], but in the projective case we do not have Galois invariant codes in general and we do not have the previous bound, nor the equality between $\mathrm{PRM}_d^{\sigma,\perp}(m)$ and $\mathrm{PRM}_d^{\perp,\sigma}(m)$.

C.4 Codes over the projective space

In this section we want to deal with the case of m variables, for $m > 2$. We have seen that, for $m = 2$, obtaining bases for the subfield subcodes is quite technical. Hence, we do not aspire to give explicit results in this section for the bases of the subfield subcodes of projective Reed-Muller codes with $m > 2$, but we can show that all the basic ideas can be generalized to treat this case. First we give a universal Gröbner basis for the vanishing ideal of P^m, which was a fundamental tool for the previous section when $m = 2$. With respect to the terminology for Gröbner bases, we refer the reader to [4]. Particular cases of the following result were already presented in [12, 19].

Theorem C.4.1. *The vanishing ideal of P^m is generated by:*

$$\begin{aligned} I(P^m) =& \langle x_0^2 - x_0, x_1^{q^s} - x_1, x_2^{q^s} - x_2, \ldots, x_m^{q^s} - x_m, (x_0-1)(x_1^2 - x_1), \\ & (x_0-1)(x_1-1)(x_2^2 - x_2), \ldots, (x_0-1)\cdots(x_{m-1}^2 - x_{m-1}), (x_0-1)\cdots(x_m-1)\rangle. \end{aligned}$$

Moreover, these generators form a universal Gröbner basis of the ideal $I(P^m)$, and we have that

$$\mathrm{in}(I(P^m)) = \langle x_0^2, x_1^{q^s}, x_2^{q^s}, \ldots, x_m^{q^s}, x_0x_1^2, x_0x_1x_2^2, \ldots, x_0x_1\cdots x_{m-1}^2, x_0x_1\cdots x_m\rangle.$$

Proof. We consider the polynomials $f_0 = x_0^2 - x_0$, $f_1 = x_1^{q^s} - x_1$, $f_2 = x_2^{q^s} - x_2$,..., $f_m = x_m^{q^s} - x_m$, and $g_1 = (x_0-1)(x_1^2 - x_1)$, $g_2 = (x_0-1)(x_1-1)(x_2^2 - x_2)$,..., $g_{m-1} =$

$(x_0-1)(x_1-1)\cdots(x_{m-2}-1)(x_{m-1}^2-x_{m-1})$, $g_m=(x_0-1)\cdots(x_m-1)$, and set $J:=\langle f_0,\ldots,f_m,g_1,\ldots,g_m\rangle$.

Due to the generators f_i, $i=0,1,\ldots,m$, it is clear that the variety defined by J over the algebraic closure $\overline{\mathbb{F}_{q^s}}$ is the same as the variety defined over $\mathbb{F}_{q^s}$. By using [11, Thm. 2.3], if we prove that the variety defined by J over $\mathbb{F}_{q^s}$ is P^m, then we can conclude that $J=I(P^m)$.

Given $P\in P^m$, we have that $P=[0:0:\cdots:0:1:P_{l+1}:\cdots:P_m]$ for some l, $0\leq l\leq m$, with $P_i\in\mathbb{F}_{q^s}$ for $i=l+1,\ldots,m$. One can check that each generator of J vanishes at P, which means that P^m is contained in the variety defined by J.

Conversely, if all the generators of J vanish at a point $P=[P_0:P_1:\cdots:P_m]$, because of the generator f_0 the first coordinate is either 0 or 1. Considering the generator g_m, we also have that

$$(P_0-1)(P_1-1)\cdots(P_m-1)=0.$$

This means that there is an integer l such that $P_l=1$, and we choose this l to be the smallest with that property. If $l=0$, then $P=[1:P_1:\cdots:P_m]\in P^m$. If $l>0$, using the generator g_{l-1} we obtain

$$(P_0-1)(P_1-1)\cdots(P_{l-1}^2-P_{l-1})=0.$$

Hence, $P_{l-1}=0$ since $P_0,P_1,\ldots,P_{l-1}$ are different from 1 due to the choice of l. Doing this recursively we get that $P_0=P_1=\cdots=P_{l-1}=0$, which means that $P=[0:0:\cdots:0:1:P_{l+1}:\cdots:P_m]\in P^m$. Therefore, we have $J=I(P^m)$.

The only thing left to prove is that the generators of $I(P^m)$ form a universal Gröbner basis for $I(P^m)$. For any monomial order we have that $x_i>1$, $i=0,1,\ldots,m$. Looking at each generator, we see that its initial monomial does not depend on the monomial order. Thus, if we prove that all the S-polynomials reduce to 0, and these reductions do not depend on the monomial order, we will have that these generators form a universal Gröbner basis for $I(P^m)$ using Buchberger's criterion [4, §9 Thm. 3, Chapter 2], and we will also obtain the stated initial ideal.

To show that all the S-polynomials reduce to 0, we will use two facts:

(a) If the leading monomials of f and g are relatively prime, then $S(f,g)$ reduces to 0 by [4, §9 Prop. 4, Chapter 2]. In particular, if f and g depend on different variables, then $S(f,g)$ reduces to 0.

(b) If f and g share a common factor w, then $S(f,g)=wS(f/w,g/w)$. Moreover, if we can apply (a) to $S(f/w,g/w)$, i.e., $S(f/w,g/w)$ reduces to 0 using f/w and g/w, then $S(f,g)$ reduces to 0 using f and g.

On one hand, for all i,j, $0\leq i<j\leq m$, we have that $S(f_i,f_j)$ reduces to 0 by (a). On the other hand, for all k,l, $1\leq k<l<m$, using (b) we have

$$S(g_k,g_l)=(x_0-1)\cdots(x_{k-1}-1)(x_k-1)S(x_k,(x_{k+1}-1)\cdots(x_{l-1}-1)(x_l^2-x_l)),$$

where the last S-polynomial reduces to 0 by (a). For $l=m$, the same argument applies, as we have

$$S(g_k,g_m)=(x_0-1)\cdots(x_{k-1}-1)(x_k-1)S(x_k,(x_{k+1}-1)\cdots(x_{m-1}-1)(x_m-1)).$$

Finally, we consider $S(f_i, g_k)$, for $1 \leq i \leq m$, $1 \leq k < m$. If $i > k$, this S-polynomial reduces to 0 by (a). If $i = k$, using (b) we have

$$S(f_k, g_k) = (x_k^2 - x_k)S((1 + x_k + \cdots + x_k^{q^s-2}), (x_1 - 1)\cdots(x_{k-1} - 1)),$$

and the last S-polynomial reduces to 0 by (a). If $i < k$, applying (b) we obtain

$$\begin{aligned} &S(f_i, g_k) = \\ &\quad (x_i - 1)S(x_i(1 + x_i + \cdots + x_i^{q^s-2}), (x_1 - 1)\cdots(x_{i-1} - 1)(x_{i+1} - 1)\cdots(x_k^2 - x_k)), \end{aligned}$$

where the last S-polynomial reduces to 0 by (a). For the cases with $i = 0$ or $k = m$, an analogous reasoning proves that the S-polynomials reduce to 0. □

Remark C.4.2. If $q^s > 2$, from the proof of Theorem C.4.1 we also obtain that the universal Gröbner basis obtained in Theorem C.4.1 is in fact the reduced Gröbner basis with respect to any monomial order. Moreover, the same happens for any subset of the generators given in Theorem C.4.1 and the ideal that they generate.

Now we give a convenient basis for $S/I(P^m)$, and also we show how to express any monomial in $S/I(P^m)$ in terms of this basis, i.e., we give the result of using the division algorithm for any monomial with respect to the universal Gröbner basis from Theorem C.4.1.

Lemma C.4.3. *The set given by the classes of the following monomials*

$$\{x_1^{a_1}\cdots x_m^{a_m}, x_0x_2^{a_2}\cdots x_m^{a_m}, \ldots, x_0x_1\cdots x_{m-2}x_m^{a_m}, x_0\cdots x_{m-1} \mid 0 \leq a_i \leq q^s - 1, 1 \leq i \leq m\}$$

is a basis for $S/I(P^m)$.

Proof. Let $\mathcal{M}$ be the given set of monomials. We have that there is no monomial from $\mathcal{M}$ contained in $\mathrm{in}(I(P^m))$ by Theorem C.4.1. We also have that $|\mathcal{M}| = q^{sm} + q^{s(m-1)} + \cdots + q^s + 1 = \frac{q^{s(m+1)}-1}{q^s-1} = |P^m|$, which is the dimension of $S/I(P^m)$ as a vector space (by definition, this is equal to $\deg(S/I(P^m))$, which is equal to $|P^m|$ by [16, Prop. 2.2]). We finish the proof by noting that the classes of the monomials not contained in $\mathrm{in}(I(P^m))$ form a basis for $S/I(P^m)$ [6, Thm. 15.3]. □

Lemma C.4.4. *Let $x_0^{a_0}x_1^{a_1}\cdots x_m^{a_m} = \prod_{i=0}^m x_i^{a_i}$ such that $a_0 > 0, a_1 > 0, \ldots, a_l > 0$ and $a_{l+1} = 0$, with $0 \leq l \leq m$ ($a_k := 0$ for $k > m$). Assume also that $a_i \leq q^s - 1$, $1 \leq i \leq m$.*

(a) If $l < m$, then

$$\begin{aligned} \prod_{i=0}^m x_i^{a_i} \equiv &\left(\prod_{i=l+2}^m x_i^{a_i}\right)\left(\prod_{i=1}^l x_i^{a_i}\right. \\ &\left. +(x_0 - 1)\left(+ (x_1 - 1)\left(\cdots \left(x_l^{a_l} + (x_{l-1} - 1)x_l \right) \cdots \right) \right) \right) \bmod I(P^m), \end{aligned}$$

where we understand that the product from s to t with $s > t$ is equal to 1.

(b) If $l = m$, then

$$\prod_{i=0}^{m} x_i^{a_i} \equiv \left(\prod_{i=1}^{m} x_i^{a_i} + (x_0 - 1)\left(\prod_{i=2}^{m} x_i^{a_i} + (x_1 - 1)\left(\cdots\left(x_m^{a_m} + (x_{m-1} - 1)\right)\cdots\right)\right)\right) \bmod I(P^m).$$

Proof. Two polynomials belong to the same class in $S/I(P^m)$ if and only if their evaluation in P^m is the same. Thus, to check the stated equivalences, it is enough to verify that both sides have the same evaluation in P^m. We assume first that $l < m$. We claim that

$$\prod_{i=0}^{l} x_i^{a_i} \equiv \prod_{i=1}^{l} x_i^{a_i} + (x_0 - 1)\left(\prod_{i=2}^{l} x_i^{a_i} + (x_1 - 1)\left(\cdots\left(x_l^{a_l} + (x_{l-1} - 1)x_l\right)\cdots\right)\right) \bmod I(P^m).$$

Indeed, if we decompose P^m as in the proof of Lemma C.2.6, we can check that the evaluation of both sides is the same at each A_r, $0 \leq r \leq m$. Because of the assumption $a_0 > 0$, the left hand side is 0 at every point which is not in A_0. Both sides evaluate to the same values in A_0. For the evaluation in A_r, with $1 \leq r < l$, we can set $x_0 = x_1 = \cdots = x_{r-1} = 0$, and in the right hand side we get

$$(-1)^{r+1}\left(\prod_{i=r}^{l} x_i^{a_i} - \left(\prod_{i=r+1}^{l} x_i^{a_i} + (x_r - 1)\left(\cdots\left(x_l^{a_l} + (x_{l-1} - 1)x_l\right)\cdots\right)\right)\right).$$

Setting $x_r = 1$, we obtain 0, which is what we get in the left hand side as well. If $r = l$, when we set $x_0 = x_1 = \cdots = x_{l-1} = 0$ we obtain

$$(-1)^{l+1}\left(x_l^{a_l} - x_l\right),$$

which is equal to 0 when we set $x_l = 1$, as the left hand side. For A_r with $l < r \leq m$, the right hand side is always 0 since it is divisible by x_l. Now (a) follows by considering the following factorization:

$$\prod_{i=0}^{m} x_i^{a_i} = \left(\prod_{i=l+2}^{m} x_i^{a_i}\right)\left(\prod_{i=0}^{l} x_i^{a_i}\right).$$

An analogous argument shows that, when $l = m$, the polynomial stated in (b) has the same evaluation as $\prod_{i=0}^{m} x_i^{a_i}$ in P^m. □

Remark C.4.5. It is not hard to see that all the monomials appearing in the right hand side of the expressions given in Lemma C.4.4 are part of the basis from Lemma C.4.3.

Hence, we have seen that the basic tools we have used for the case $m = 2$ can be generalized to the case $m > 2$. For the duals of the subfield subcodes, the reasoning that led to (C.3.1) and (C.3.2) shows that, in order to obtain a basis for $\mathcal{T}(S_d)$, for each monomial $x^\gamma \in S_d$, it is enough to consider the traces

$$\{\mathcal{T}_{\hat{\gamma}}(\xi_{\hat{\gamma}}^r x^\gamma) \mid 0 \leq r \leq n_{\hat{\gamma}} - 1\}, \tag{C.4.1}$$

where in this case we are considering cyclotomic sets in m coordinates, and we extend the definitions for $\hat{\gamma}$ and $\mathcal{T}_{\hat{\gamma}}$ to this case in the obvious way. Hence, to obtain a basis we have to extract a maximal linearly independent set from the union of the previous sets. Theorem C.4.1 and Lemma C.4.4 give the necessary tools to do that, but getting a general explicit formula for such a basis is quite involved.

For the primary code, the idea would be to consider homogenizations of the traces from the basis of the affine case from Theorem C.2.3, and then consider linear combinations of these polynomials such that, when setting $x_0 = x_1 = \cdots = x_j = 0$ for some $0 \leq j \leq m-1$, we obtain traces in less variables, similarly to what we did in the case of the projective plane.

C.5 Examples

In this section we show some examples of the parameters obtained from subfield subcodes of projective Reed-Muller codes over the projective plane. For computing the dimension, we can use Corollary C.3.13 and Corollary C.3.42, and for computing the minimum distance we use Magma [2]. We will denote the parameters of $\mathrm{PRM}_d^\sigma(2)$ by $[n, k, \delta]$, and the parameters of the dual code $\mathrm{PRM}_d^{\sigma,\perp}(2)$ by $[n, k^\perp, \delta^\perp]$. With respect to the parameters of the codes that we obtain, it is only possible to compare these codes with the codes from [13] for small finite field sizes. This is because the codes that we obtain have length $n = \frac{q^{3s}-1}{q^s-1} = q^{2s} + q^s + 1$, which gives rise to very long codes when we increase q or s. Moreover, it is better to consider moderate values of s due to the fact that the size of the corresponding cyclotomic sets increases for larger s, and therefore if we start with degree d and we consider degree $d-1$, for each monomial of degree d that we are no longer evaluating, all its powers of q (seen in $S/I(P^2)$) will not appear in any trace from the basis that we have given for $\mathrm{PRM}_d^\sigma(2)$, and the size of the set formed by the monomial and its powers of q is precisely the size of the corresponding cyclotomic set. This can cause significant drops in dimension, leading in some cases to codes with worse parameters compared to the cases with smaller s. Thus, we first consider binary codes and ternary codes arising from extensions of small degree.

For the extensions $\mathbb{F}_4 \supset \mathbb{F}_2$ and $\mathbb{F}_8 \supset \mathbb{F}_2$, we obtain the parameters from Table C.1. For the extension $\mathbb{F}_8 \supset \mathbb{F}_2$ we omit the codes with $d = 2, 3$ as they are equal to $\mathrm{PRM}_1^\sigma(2)$. In the cases where $\delta^\perp$ is 1, we have that $\mathrm{PRM}_d(2)$ is a degenerate code. For instance, for the extension $\mathbb{F}_4 \supset \mathbb{F}_2$, for $d = 1$ we have $q^s + 1 = 5$ common zeroes for all the vectors in the code, which means that, after puncturing, we obtain the same as the subfield subcode of an affine Reed-Muller code. However, for $d = 2$ we only have 1 common zero, and the corresponding code after puncturing does not correspond to the subfield subcode of any affine Reed-Muller code. With respect to the parameters, some of the codes from Table C.1 have the best known parameters for a linear code with its length and dimension, according to [13]. For example, that is the case for the codes with parameters $[21, 9, 8]_2$, $[21, 12, 5]_2$ and $[21, 16, 3]_2$.

With respect to ternary codes, we consider the extension $\mathbb{F}_9 \supset \mathbb{F}_3$. The parameters of the corresponding codes are presented in Table C.2, where we have omitted the case $d = 2$ since it corresponds to the same code as $\mathrm{PRM}_1^\sigma(2)$.

We can compare the parameters of these codes with the ones obtained with affine Reed-Muller codes. Besides the fact that we obtain longer codes for the same field size, if we

Table C.1: Binary codes corresponding to the extensions $\mathbb{F}_4 \supset \mathbb{F}_2$ and $\mathbb{F}_8 \supset \mathbb{F}_2$, respectively.

d	n	k	δ	$k^\perp$	$\delta^\perp$
1	21	1	16	20	1
2	21	2	12	19	1
3	21	9	8	12	5
4	21	11	4	10	2
5	21	16	3	5	8
6	21	20	2	1	21

d	n	k	δ	$k^\perp$	$\delta^\perp$
1	73	1	64	72	1
4	73	2	40	71	1
5	73	7	32	66	1
6	73	8	24	65	1
7	73	27	16	46	9
8	73	28	8	45	1
9	73	32	8	41	2
10	73	40	8	33	1
11	73	51	5	22	16
12	73	59	4	14	4
13	73	66	3	7	32
14	73	72	2	1	73

Table C.2: Ternary codes corresponding to the extension $\mathbb{F}_9 \supset \mathbb{F}_3$.

d	n	k	δ	$k^\perp$	$\delta^\perp$
1	91	1	81	90	1
3	91	2	63	89	1
4	91	9	54	82	4
5	91	9	45	82	1
6	91	10	36	81	1
7	91	19	27	72	1
8	91	36	18	55	10
9	91	38	9	53	2
10	91	45	9	46	4
11	91	58	7	33	18
12	91	70	6	21	36
13	91	73	5	18	6
14	91	80	4	11	36
15	91	86	3	5	54
16	91	90	2	1	91

consider $\frac{k+\delta}{n}$ as a measure of how good a code is, we usually have that the projective code $\mathrm{PRM}_d^\sigma(2)$ is better in that sense than $\mathrm{RM}_d^\sigma(2)$. For example, we have that the code $\mathrm{RM}_4^\sigma(2)$ corresponding to the extension $\mathbb{F}_9 \supset \mathbb{F}_3$ has parameters $[81, 9, 45]_3$, and $\mathrm{PRM}_4^\sigma(2)$ has parameters $[91, 9, 54]_3$, and one can check that $\mathrm{PRM}_4^\sigma(2)$ has better parameters with respect to the value $\frac{k+\delta}{n}$. In fact, the parameters of the code $\mathrm{PRM}_4^\sigma(2)$ are the best known parameters for a code with length 91 and dimension 9 over $\mathbb{F}_3$, according to [13]. Moreover, the codes from Table C.2 with parameters $[91, 21, 36]_3$, $[91, 82, 4]_3$ and $[91, 86, 3]_3$ are also the best known according to [13].

For extensions of higher degree, or for fields with higher q, the codes that we obtain in this way are too long to be compared to the ones from [13]. As we have seen in the

previous examples, some of the codes that we obtain have the best known parameters, while others do not have great parameters. Focusing on the ones with better parameters, in Table C.3 we provide some long codes that surpass the Gilbert-Varshamov bound for different field extensions. For the minimum distance, we use the bound (C.3.12) since these codes are too large for Magma [2].

Table C.3: Long codes exceeding the Gilbert-Varshamov bound.

q	s	d	n	k	$\delta \geq$
2	4	28	273	255	4
2	4	29	273	264	3
4	2	5	273	9	192
4	2	28	273	262	4
4	2	29	273	268	3
5	2	6	651	9	500
5	2	46	651	640	4
5	2	47	651	646	3
3	3	50	757	741	4
3	3	51	757	750	3
2	5	60	1057	1035	4
2	5	61	1057	1046	3
7	2	8	2451	9	2058
7	2	94	2451	2440	4
7	2	95	2451	2446	3

Finally, for the case $m > 2$, in Table C.4 we show the binary codes obtained by considering the subfield subcodes of projective Reed-Muller codes over $\mathbb{P}^3$ with respect to the extension $\mathbb{F}_4 \supset \mathbb{F}_2$, where we have computed the parameters with Magma [2]. The codes with parameters $[85, 16, 32]_2$, $[85, 60, 8]_2$ and $[85, 78, 3]_2$ have the best known parameters according to [13].

Table C.4: Binary codes corresponding to the extension $\mathbb{F}_4 \supset \mathbb{F}_2$ with $m = 3$.

d	n	k	δ	$k^\perp$	$\delta^\perp$
1	85	1	64	84	1
2	85	2	48	83	1
3	85	16	32	69	5
4	85	18	16	67	1
5	85	33	12	52	2
6	85	60	8	25	21
7	85	67	4	18	8
8	85	78	3	7	32
9	85	84	2	1	85

Bibliography

[1] J. Bierbrauer. The theory of cyclic codes and a generalization to additive codes. *Des. Codes Cryptogr.*, 25(2):189–206, 2002.

[2] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[3] S. D. Cohen. Primitive elements and polynomials with arbitrary trace. *Discrete Math.*, 83(1):1–7, 1990.

[4] D. A. Cox, J. Little, and D. O'Shea. *Ideals, varieties, and algorithms*. Undergraduate Texts in Mathematics. Springer, Cham, fourth edition, 2015. An introduction to computational algebraic geometry and commutative algebra.

[5] P. Delsarte. On subfield subcodes of modified Reed-Solomon codes. *IEEE Trans. Inform. Theory*, IT-21(5):575–576, 1975.

[6] D. Eisenbud. *Commutative algebra*, volume 150 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1995. With a view toward algebraic geometry.

[7] C. Galindo, O. Geil, F. Hernando, and D. Ruano. On the distance of stabilizer quantum codes from J-affine variety codes. *Quantum Inf. Process.*, 16(4):Paper No. 111, 32, 2017.

[8] C. Galindo, O. Geil, F. Hernando, and D. Ruano. New binary and ternary LCD codes. *IEEE Trans. Inform. Theory*, 65(2):1008–1016, 2019.

[9] C. Galindo and F. Hernando. Quantum codes from affine variety codes and their subfield-subcodes. *Des. Codes Cryptogr.*, 76(1):89–100, 2015.

[10] C. Galindo, F. Hernando, and D. Ruano. Stabilizer quantum codes from J-affine variety codes and a new Steane-like enlargement. *Quantum Inf. Process.*, 14(9):3211–3231, 2015.

[11] S. R. Ghorpade. A note on Nullstellensatz over finite fields. In *Contributions in algebra and algebraic geometry*, volume 738 of *Contemp. Math.*, pages 23–32. Amer. Math. Soc., 2019.

[12] P. Gimenez, D. Ruano, and R. San-José. Entanglement-assisted quantum error-correcting codes from subfield subcodes of projective Reed-Solomon codes. *Comput. Appl. Math.*, 42(8):Paper No. 363, 31, 2023.

[13] M. Grassl. Bounds on the minimum distance of linear codes and quantum codes. Online available at `http://www.codetables.de`, 2007. Accessed on 2023-04-04.

[14] F. Hernando, M. E. O'Sullivan, E. Popovici, and S. Srivastava. Subfield-subcodes of generalized toric codes. In *2010 IEEE International Symposium on Information Theory*, pages 1125–1129, 2010.

[15] W. C. Huffman and V. Pless. *Fundamentals of error-correcting codes*. Cambridge University Press, Cambridge, 2003.

[16] D. Jaramillo, M. Vaz Pinto, and R. H. Villarreal. Evaluation codes and their basic parameters. *Des. Codes Cryptogr.*, 89(2):269–300, 2021.

[17] G. Lachaud. The parameters of projective Reed-Muller codes. *Discrete Math.*, 81(2):217–221, 1990.

[18] D.-J. Mercier and R. Rolland. Polynômes homogènes qui s'annulent sur l'espace projectif $\mathrm{P}^m(\mathbf{F}_q)$. *J. Pure Appl. Algebra*, 124(1-3):227–240, 1998.

[19] N. Nakashima and H. Matsui. Decoding of projective reed-muller codes by dividing a projective space into affine spaces. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, E99.A(3):733–741, 2016.

[20] A. B. Sørensen. Projective Reed-Muller codes. *IEEE Trans. Inform. Theory*, 37(6):1567–1576, 1991.

Paper D

A recursive construction for projective Reed-Muller codes

Rodrigo San-José

Abstract

We give a recursive construction for projective Reed-Muller codes in terms of affine Reed-Muller codes and projective Reed-Muller codes in fewer variables. From this construction, we obtain the dimension of the subfield subcodes of projective Reed-Muller codes for some particular degrees that give codes with good parameters. Moreover, from this recursive construction we derive a lower bound for the generalized Hamming weights of projective Reed-Muller codes which is sharp in most of the cases we have checked.

Keywords: Projective Reed-Muller codes, recursive construction, subfield subcodes, generalized Hamming weights.

MSC: 94B05, 11T71, 14G50

DOI: 10.48550/arXiv.2312.05072

Reference: R. San-José. A recursive construction for projective Reed-Muller codes. IEEE Transactions on Information Theory, to appear (2024). ArXiv 2312.05072.

Affiliation: Rodrigo San-José: IMUVA-Mathematics Research Institute, Universidad de Valladolid.

D.1 Introduction

Binary affine Reed-Muller codes can be constructed recursively via the $(u \mid u+v)$ construction, and, more generally, q-ary affine Reed-Muller codes can be constructed recursively using the matrix-product code construction [5, Thm 5.6]. These recursive constructions provide a wealth of information about the code. For example, the recursive construction from [5] provides a simple proof for the minimum distance of affine Reed-Muller codes. Moreover, the subfield subcode of a code obtained using the $(u \mid u+v)$ construction can be obtained by applying the $(u \mid u+v)$ construction to the subfield subcodes of the component codes. In this work we are interested in a recursive construction for projective Reed-Muller codes, a generalization of affine Reed-Muller codes obtained by evaluating homogeneous polynomials in the projective space $\mathbb{P}^m$ which was introduced by Lachaud [18] and whose basic parameters are presented in full generality in [20]. We apply this recursive construction to obtain information about the subfield subcodes and generalized Hamming weights of projective Reed-Muller codes.

Given a code $C \subset \mathbb{F}_{q^s}^n$, its subfield subcode with respect to the extension $\mathbb{F}_{q^s} \supset \mathbb{F}_q$ is the linear code $C \cap \mathbb{F}_q^n$. This is a standard procedure that has been used to construct long linear codes over a small finite field. In particular, this technique has been applied to obtain BCH codes as subfield subcodes of Reed-Solomon codes [4], and in the multivariate case, the subfield subcodes of J-affine variety codes (in particular, affine Reed-Muller codes) are well known and have been applied in several contexts [10–12]. The subfield subcodes of projective Reed-Solomon codes and projective Reed-Muller codes were studied in [13] and [14], respectively. The primary challenge when dealing with subfield subcodes is the computation of a basis for the code, which, in particular, gives the dimension of the subfield subcode. However, one can check in [14] that, for $m = 2$, the expressions for the basis of the subfield subcode get quite involved, and for $m > 2$, obtaining explicit expressions for the basis in general seems out of reach. In Section D.4, we show that, for certain degrees, the recursive construction we obtain for projective Reed-Muller codes can be applied to their subfield subcodes as well. This directly gives the dimension of these subfield subcodes in a recursive manner, for any $m \geq 2$. Moreover, an explicit expression for a basis of these subfield subcodes can be obtained in terms of the basis from the subfield subcodes of affine Reed-Muller codes and the subfield subcodes of projective Reed-Muller codes with fewer variables. We also show that these particular degrees give codes with good parameters.

With respect to the generalized Hamming weights of a code, these are a set of parameters that generalize the minimum distance of a code. One of the main applications of the generalized Hamming weights is that they characterize the performance of the code on the wire-tap channel of type II [21]. The generalized Hamming weights of affine Reed-Muller codes were completely determined more than 20 years ago in [16]. However, the computation of the generalized Hamming weights of projective Reed-Muller codes in general remains an open problem and only partial results are known [1, 6, 8]. In [3], many of the previous results and hypotheses are collected, and the authors obtain the generalized Hamming weights of projective Reed-Muller codes in some cases for degree $d < q^s$. In Section D.5, we use the recursive construction from Section D.3 in order to give a recursive lower bound for the generalized Hamming weights of a projective Reed-Muller code of any degree. Moreover, we also provide an upper bound that gives us a criterion to ensure that the bound is sharp in many cases. In the particular case of $m = 2$, we are able to give a

more explicit expression for these bounds. By considering the general properties of generalized Hamming weights and our bounds, we obtain the exact values of the generalized Hamming weights of projective Reed-Muller codes in many cases.

D.2 Preliminaries

We consider the finite field $\mathbb{F}_q$ of q elements with characteristic p, and its degree s extension $\mathbb{F}_{q^s}$, with $s \geq 1$. We consider the projective space $\mathbb{P}^m$ over $\mathbb{F}_{q^s}$. We denote by p_j the number of points in $\mathbb{P}^j$, i.e., $p_j = \frac{q^{s(j+1)}-1}{q^s-1} = q^{sj} + q^{s(j-1)} + \cdots + 1$. Throughout this work, we will fix representatives for the points of $\mathbb{P}^m$: for each point $[Q] \in \mathbb{P}^m$, we choose the representative whose first nonzero coordinate is equal to 1. We will denote by P^m the set of representatives that we have chosen (seen as points in the affine space $\mathbb{A}^{m+1}$). Therefore, we have the following decomposition

$$P^m = \left(\{1\} \times \mathbb{F}_{q^s}^m\right) \cup \left(\{0\} \times \{1\} \times \mathbb{F}_{q^s}^{m-1}\right) \cup \cdots \cup \{(0, \ldots, 0, 1)\}.$$

Moreover, we also can obtain this recursively by noting that

$$P^m = \left(\{1\} \times \mathbb{F}_{q^s}^m\right) \cup \left(\{0\} \times P^{m-1}\right). \tag{D.2.1}$$

We consider now the polynomial ring $S = \mathbb{F}_{q^s}[x_0, \ldots, x_m]$. Let $n = |P^m| = p_m$. We define the following evaluation map:

$$\mathrm{ev} : S \to \mathbb{F}_{q^s}^n, \;\; f \mapsto (f(Q_1), \ldots, f(Q_n))_{Q_i \in P^m}.$$

Let d be a positive integer. If we consider $S_d \subset S$, the set of homogeneous polynomials of degree d, we have that $\mathrm{ev}(S_d)$ is the projective Reed-Muller code of degree d, which we will denote by $\mathrm{PRM}_d(q^s, m)$, or $\mathrm{PRM}_d(m)$ if there is no confusion about the field. For $m = 1$, we obtain the projective Reed-Solomon codes (sometimes called doubly extended Reed-Solomon codes), which are MDS codes with parameters $[q^s + 1, d + 1, q^s - d + 1]$. For a code $C \subset \mathbb{F}_q^n$, we will denote its minimum distance by $d_1(C)$ (using the notation for generalized Hamming weights that we will consider in Section D.5). For the case $m \geq 2$, we have the following results from [20] about the parameters of projective Reed-Muller codes and their duality.

Theorem D.2.1. *The projective Reed-Muller code* $\mathrm{PRM}_d(q^s, m)$, $1 \leq d \leq m(q^s - 1)$, *is an* $[n, k]$*-code with*

$$n = \frac{q^{s(m+1)} - 1}{q^s - 1},$$
$$k = \sum_{t \equiv d \bmod q^s - 1, 0 < t \leq d} \left(\sum_{j=0}^{m+1} (-1)^j \binom{m+1}{j} \binom{t - jq^s + m}{t - jq^s} \right).$$

For the minimum distance, we have

$$d_1(\mathrm{PRM}_d(q^s, m)) = (q^s - \mu) q^{s(m-\nu-1)}, \;\; \textit{where} \;\; d - 1 = \nu(q^s - 1) + \mu, \; 0 \leq \mu < q^s - 1.$$

Theorem D.2.2. *Let $1 \leq d \leq m(q^s-1)$ and let $d^\perp = m(q^s-1) - d$. Then*

$$\begin{aligned} \mathrm{PRM}_d^\perp(q^s, m) &= \mathrm{PRM}_{d^\perp}(q^s, m) && \text{if } d \not\equiv 0 \bmod (q^s-1), \\ \mathrm{PRM}_d^\perp(q^s, m) &= \mathrm{PRM}_{d^\perp}(q^s, m) + \langle (1, \ldots, 1) \rangle && \text{if } d \equiv 0 \bmod (q^s-1). \end{aligned}$$

Let $d > 0$ and let $M_i = \{x_i^{\alpha_i} \cdots x_m^{\alpha_m}, |\alpha| = d, \alpha_i > 0, 0 \leq \alpha_j \leq q^s - 1, i < j \leq m\}$, for $i = 0, 1, \ldots, m$, and $M = \bigcup_{i=0}^m M_i$. One can check that M is a basis for $S_d/I(\mathbb{P}^m)_d \cong \mathrm{PRM}_d(m)$ (for example, see [2]), where $I(\mathbb{P}^m)$ is the vanishing ideal of $\mathbb{P}^m$, i.e, the ideal generated by the homogeneous polynomials that vanish at all the points of $\mathbb{P}^m$. This also implies that the image by the evaluation map of M is a basis for $\mathrm{PRM}_d(m)$.

We will also need to use affine Reed-Muller codes, which we denote by $\mathrm{RM}_d(q^s, m)$, or simply $\mathrm{RM}_d(m)$ if there is no confusion about the field. We consider the evaluation map

$$\mathrm{ev}_{\mathbb{A}} : R \to \mathbb{F}_{q^s}^{q^{ms}}, \ \ f \mapsto (f(Q_1), \ldots, f(Q_n))_{Q_i \in \mathbb{F}_{q^s}^m},$$

where $R = \mathbb{F}_{q^s}[x_1, \ldots, x_m]$. Let $R_{\leq d}$ be the polynomials of R with degree less than or equal to d. Then we have $\mathrm{RM}_d(m) := \mathrm{ev}_{\mathbb{A}}(R_{\leq d})$. The following result about the parameters of affine Reed-Muller codes appears in [9, 17].

Theorem D.2.3. *The Reed-Muller code $\mathrm{RM}_d(q^s, m)$, $1 \leq d \leq m(q^s-1)$, is an $[n, k]$-code with*

$$\begin{aligned} n &= q^{sm}, \\ k &= \sum_{t=0}^{d} \sum_{j=0}^{m} (-1)^j \binom{m}{j} \binom{t - jq^s + m - 1}{t - jq^s}. \end{aligned}$$

For the minimum distance, we have

$$d_1(\mathrm{RM}_d(q^s, m)) = (q^s - \mu) q^{s(m-\nu-1)}, \ \text{where} \ \ d = \nu(q^s-1) + \mu, \ 0 \leq \mu < q^s - 1.$$

D.3 A recursive construction for projective Reed-Muller codes

In this section, we introduce a recursive construction for projective Reed-Muller codes from affine Reed-Muller codes and projective Reed-Muller codes over a smaller projective space. The inspiration behind this idea was the fact that affine Reed-Muller codes can be obtained recursively by using matrix-product codes [5, Thm. 5.6].

In order to state this recursive construction, we need to consider a specific ordering of the points in P^m: we are going to assume that the first q^{sm} points of P^m are the points of $(\{1\} \times \mathbb{F}_{q^s}^m)$ (see decomposition (D.2.1)). Therefore, we have that the first q^{sm} coordinates of the evaluation of a polynomial in P^m correspond to the evaluation at the points $(\{1\} \times \mathbb{F}_{q^s}^m)$, and the rest of coordinates correspond to the evaluation at the points in the second part of the decomposition (D.2.1). Let $\xi \in \mathbb{F}_{q^s}$ be a primitive element. We are also going to consider the following decomposition

$$\mathbb{F}_{q^s}^m = P^{m-1} \cup \xi \cdot P^{m-1} \cup \cdots \cup \xi^{q^s-2} \cdot P^{m-1} \cup \{(0, \ldots, 0)\}. \tag{D.3.1}$$

This decomposition is obtained by noting the following: given a point Q in $\mathbb{F}_{q^s}^m \setminus \{(0,\dots,0\}$, its first nonzero coordinate is equal to ξ^r for some $0 \leq r \leq q^s - 2$, which implies that $Q \in \xi^r \cdot P^{m-1}$. Therefore, using (D.2.1) and (D.3.1) we have

$$P^m = \left(\{1\} \times \left(P^{m-1} \cup \xi \cdot P^{m-1} \cup \cdots \cup \xi^{q^s-2} \cdot P^{m-1} \cup \{(0,\dots,0)\}\right)\right) \cup \left(\{0\} \times P^{m-1}\right). \tag{D.3.2}$$

We fix an ordering $\{Q'_1, \dots, Q'_{p_{m-1}}\}$ of the points of P^{m-1}. We are going to assume that the first p_{m-1} coordinates of the image of the evaluation map correspond to the evaluation at the points $\{1\} \times P^{m-1}$ (with the fixed ordering for P^{m-1}), the following p_{m-1} coordinates correspond to the evaluation at the points $\{1\} \times \xi \cdot P^{m-1}$, etc. We fix this for all the points in $\{1\} \times \mathbb{F}_{q^s}^m$, and for the rest of the coordinates, which correspond to the evaluation in $\{0\} \times P^{m-1}$, we also assume that we are using the same fixed ordering for P^{m-1}.

Hence, for a given ordering of the points of P^{m-1}, we fix the ordering of all the points of P^m as shown above. In what follows, we assume that the projective Reed-Muller codes are obtained by using the evaluation map over P^m with this ordering for the points, and the affine Reed-Muller codes are obtained by evaluating in $\mathbb{F}_{q^s}^m$, ordered in the same way that we ordered $\{1\} \times \mathbb{F}_{q^s}^m$.

Theorem D.3.1. *Let $1 \leq d \leq m(q^s - 1)$ and let ξ be a primitive element in $\mathbb{F}_{q^s}$. We have the following recursive construction:*

$$\mathrm{PRM}_d(m) = \{(u + v_{\xi,d}, v) \mid u \in \mathrm{RM}_{d-1}(m), v \in \mathrm{PRM}_d(m-1)\},$$

where $v_{\xi,d} := v \times \xi^d v \times \cdots \times \xi^{(q^s-2)d} v \times \{0\} = (v, \xi^d v, \xi^{2d} v, \dots, \xi^{(q^s-2)d} v, 0)$.

Proof. Taking into account that x_0 divides all the monomials in M_0 and the decomposition (D.2.1), it is clear that $\langle \mathrm{ev}(M_0) \rangle = \mathrm{RM}_{d-1}(m) \times \{0\}^{p_{m-1}}$.

Now we consider a monomial $x^\alpha \in \bigcup_{i=1}^m M_i$. Its evaluation in $\{0\} \times P^{m-1}$ (the second part of the decomposition (D.2.1)) is in $\mathrm{PRM}_d(m-1)$ because x^α only involves the last m variables. In fact, the evaluation of all the monomials in $\bigcup_{i=1}^m M_i$ at the points of $\{0\} \times P^{m-1}$ gives a basis for $\mathrm{PRM}_d(m-1)$. Now assume that the evaluation of x^α at the points $\{0\} \times P^{m-1}$ is v. Let $\xi \in \mathbb{F}_{q^s}$ be a primitive element. Then, because of the ordering that we have chosen and the decomposition (D.3.1), it is clear that the evaluation of x^α at the points $\{1\} \times \mathbb{F}_{q^s}^m$ is precisely $v_{\xi,d}$. We have obtained the evaluation of the monomial x^α at both parts of the decomposition (D.2.1). Thus, $\mathrm{ev}(x^\alpha) = (v_{\xi,d}, v)$.

If we have $f \in k[x_0, \dots, x_m]_d / I(\mathbb{P}^m)_d \cong \mathrm{PRM}_d(m)$, then it can be written as

$$f = \sum_i \lambda_i b_i + \sum_i \gamma_i a_i, b_i \in M_0, a_i \in \bigcup_{i=1}^m M_i, \lambda_i, \gamma_i \in \mathbb{F}_{q^s}.$$

We have seen that $\mathrm{ev}(b_i) = u \times \{0\}^{p_{m-1}}$, for some $u \in \mathrm{RM}_{d-1}(m)$, and $\mathrm{ev}(a_i) = (v_{\xi,d}, v)$, for some $v \in \mathrm{PRM}_d(m-1)$. We finish the proof by considering the linearity of the evaluation map. □

Remark D.3.2. For $d \equiv 0 \bmod q^s - 1$, the construction is simpler and, to some extent, resembles the $(u \mid u + v)$ construction:

$$\mathrm{PRM}_d(m) = \{(u + v_{\xi,d}, v), u \in \mathrm{RM}_{d-1}(m), v \in \mathrm{PRM}_d(m-1)\},$$

with $v_{\xi,d} = (v, v, \dots, v, 0)$.

With the construction from Theorem D.3.1 we can recover the dimension of projective Reed-Muller codes from Theorem D.2.1 in a different way, which was already noted in [19, Lem. 9].

Corollary D.3.3. *We have that*

$$\dim(\mathrm{PRM}_d(m)) = \dim(\mathrm{RM}_{d-1}(m)) + \dim(\mathrm{PRM}_d(m-1)).$$

Proof. Using the notation in Theorem D.3.1, we have $\dim(\mathrm{RM}_{d-1}(m))$ linearly independent vectors corresponding to $v = 0$, and we have $\dim(\mathrm{PRM}_d(m-1))$ linearly independent vectors corresponding to $u = 0$. By the construction from Theorem D.3.1, every codeword of $\mathrm{PRM}_d(m)$ can be obtained as the sum of a vector with $u = 0$ and a vector with $v = 0$, and we obtain the result. □

D.4 Subfield subcodes of projective Reed-Muller codes

As we stated at the beginning of the previous section, in some cases the recursive construction from Theorem D.3.1 resembles the $(u \mid u + v)$ construction. It is not hard to check that, given two codes C_1, C_2, the subfield subcode of the resulting code after using the $(u \mid u + v)$ construction with C_1 and C_2 is equal to the code obtained by applying the $(u \mid u + v)$ construction to C_1^σ and C_2^σ. Therefore, one may wonder if we can use the construction from Theorem D.3.1 in order to obtain results about the subfield subcodes of projective Reed-Muller codes, or even a recursive construction for them, which is what we study in this section. In [14] the subfield subcodes of projective Reed-Muller codes were studied, mainly for the case $m = 2$. Our approach in this section can be applied recursively for any m, and for the case $m = 2$ our method provides an easier way to obtain the basis of the subfield subcode for some degrees. We start with a result about the minimum distance and dimension of the subfield subcodes of projective Reed-Muller codes.

Corollary D.4.1. *Let $1 \leq d \leq m(q^s - 1)$. We have the following inequalities:*

$$d_1(\mathrm{RM}_{d-1}(m)) \leq d_1(\mathrm{PRM}_d^\sigma(m)) \leq d_1(\mathrm{RM}_{d-1}^\sigma(m)),$$
$$\dim(\mathrm{PRM}_d^\sigma(m)) \geq \dim(\mathrm{RM}_{d-1}^\sigma(m)),$$

and the last inequality is strict if $\mathrm{PRM}_d^\sigma(m)$ is non-degenerate.

Proof. We have that $d_1(\mathrm{PRM}_d(m)) \leq d_1(\mathrm{PRM}_d^\sigma(m))$ because $\mathrm{PRM}_d^\sigma(m) \subset \mathrm{PRM}_d(m)$, and one can check that $d_1(\mathrm{PRM}_d(m)) = d_1(\mathrm{RM}_{d-1}(m))$ using Theorem D.2.1 and Theorem D.2.3. For the other inequalities, by Theorem D.3.1 we obtain $\mathrm{RM}_{d-1}(m) \times \{0\}^{p_{m-1}} \subset \mathrm{PRM}_d(m)$, which implies $\mathrm{RM}_{d-1}^\sigma(m) \times \{0\}^{p_{m-1}} \subset \mathrm{PRM}_d^\sigma(m)$. □

In most of the non-degenerate cases we have the equality for the three minimum distances in the previous result, although the bound is not always sharp as it was seen in [14]. In the non-degenerate case we have $\dim(\mathrm{PRM}_d^\sigma(m)) > \dim(\mathrm{RM}_{d-1}^\sigma(m))$, which may also be true in many degenerate cases, as one can check for the case $m = 2$ in [14, Cor 3.41].

For some specific degrees we are able to obtain a recursive construction for the subfield subcodes of projective Reed-Muller codes, which in turn allows us to give more precise results about the parameters.

Corollary D.4.2. *Let $\xi \in \mathbb{F}_{q^s}$ be a primitive element. Let $m > 1$ and let $d_\lambda = \lambda \frac{q^s-1}{q-1}$ for some $\lambda \in \{1, 2, \ldots, m(q-1)\}$. Then we have*

$$\mathrm{PRM}^\sigma_{d_\lambda}(m) = \{(u + v_{\xi,d_\lambda}, v), u \in \mathrm{RM}^\sigma_{d_\lambda - 1}(m), v \in \mathrm{PRM}^\sigma_{d_\lambda}(m-1)\}.$$

As a consequence, we obtain:

$$\dim(\mathrm{PRM}^\sigma_{d_\lambda}(m)) = \dim(\mathrm{RM}^\sigma_{d_\lambda - 1}(m)) + \dim(\mathrm{PRM}^\sigma_{d_\lambda}(m-1)).$$

Proof. We have that

$$(\xi^{d_\lambda})^{q-1} = \xi^{\lambda(q^s-1)} = 1 \implies \xi^{d_\lambda} \in \mathbb{F}_q.$$

Then it is clear that for any $u \in \mathrm{RM}^\sigma_{d_\lambda-1}(m)$, $v \in \mathrm{PRM}^\sigma_{d_\lambda}(m-1)$, we have $v_{\xi,d_\lambda} \in \mathbb{F}_q^n$ and $(u + v_{\xi,d_\lambda}, v) \in \mathrm{PRM}^\sigma_{d_\lambda}(m)$ because of Theorem D.3.1.

On the other hand, if we have $w \in \mathrm{PRM}^\sigma_{d_\lambda}(m)$, by Theorem D.3.1 we know that w is of the form $(u + v_{\xi,d_\lambda}, v)$, for $u \in \mathrm{RM}_{d-1}(m), v \in \mathrm{PRM}_d(m-1)$, and its coordinates are in $\mathbb{F}_q$. Therefore, v must have its coordinates in $\mathbb{F}_q$, i.e., $v \in \mathrm{PRM}^\sigma_d(m-1)$. Moreover, taking into account that $\xi^{d_\lambda} \in \mathbb{F}_q$, we also get that $v_{\xi,d_\lambda} \in \mathbb{F}_q^n$, which implies that $u \in \mathrm{RM}^\sigma_{d-1}(m)$. Arguing as in Corollary D.3.3 we obtain the formula for the dimension. □

Remark D.4.3. Note that the hypothesis about the degrees in Corollary D.4.2 is necessary. For instance, in [14, Cor. 3.41] it can be seen that the formula for the dimension from Corollary D.4.2 does not hold in general when $d \neq d_\lambda$ for any $\lambda \in \{1, 2, \ldots, m(q-1)\}$.

In all the cases from Corollary D.4.2 we can obtain a set of polynomials such that their image by the evaluation map is a basis for $\mathrm{PRM}^\sigma_{d_\lambda}(m)$ in a straightforward manner. In order to do so, for a given degree $d > 0$, we define the homogenization up to degree d of a polynomial $f \in \mathbb{F}_{q^s}[x_1, \ldots, x_m]$ with degree $\deg(f) < d$ as $f^h = x_0^d f(x_1/x_0) \in \mathbb{F}_{q^s}[x_0, \ldots, x_m]_d$. Note that, with this definition, we always have that x_0 divides f^h.

Corollary D.4.4. *Let $d_\lambda = \lambda \frac{q^s-1}{q-1}$ for some $\lambda \in \{1, 2, \ldots, m(q-1)\}$. Let $\{f_i\}_i \subset \mathbb{F}_{q^s}[x_1, \ldots, x_m]_{\leq d-1}$ (resp. $\{g_j\}_j \subset \mathbb{F}_{q^s}[x_1, \ldots, x_m]_d$) be a set of polynomials such that their evaluation in $\mathbb{F}_{q^s}^m$ (resp. P^{m-1}) is a basis for $\mathrm{RM}^\sigma_{d-1}(m)$ (resp. $\mathrm{PRM}^\sigma_d(m-1)$). Then the image by the evaluation map of $\{f_i^h\}_i \cup \{g_j\}_j \subset \mathbb{F}_{q^s}[x_0, \ldots, x_m]$ over P^m is a basis for $\mathrm{PRM}^\sigma_d(m)$.*

Proof. Assume that we have the sets $\{f_i\}_i$ and $\{g_j\}_j$ as in the statement. Then we have that $\{f_i^h\}_i$ is a set of homogeneous polynomials of degree d, and the image by the evaluation map of this set generates $\mathrm{RM}^\sigma_{d-1}(m) \times \{0\}^{p_{m-1}}$, i.e., the vectors with $v = 0$ of the recursive construction from Corollary D.4.2.

Let $\xi \in \mathbb{F}_{q^s}$ be a primitive element. If the evaluation of a polynomial of $\{g_j\}_j$ over P^{m-1} is $v \in \mathrm{PRM}^\sigma_d(m-1)$, then, when regarding this polynomial in $\mathbb{F}_{q^s}[x_0, \ldots, x_m]$, the evaluation over P^m is precisely $(v_{\xi,d}, v)$ (this is the idea of the proof of Theorem D.3.1). Therefore, the image by the evaluation map of $\{f_i^h\}_i \cup \{g_j\}_j$ over P^m generates

$$\{(u + v_{\xi,d_\lambda}, v), u \in \mathrm{RM}^\sigma_{d_\lambda - 1}(m), v \in \mathrm{PRM}^\sigma_{d_\lambda}(m-1)\},$$

which is $\mathrm{PRM}^\sigma_d(m)$ by Corollary D.4.2. □

In both Corollary D.4.2 and Corollary D.4.4, in order to use the recursion we need to obtain bases for affine and projective Reed-Muller codes for some $m \geq 1$. Sets of polynomials whose evaluation are a basis for the subfield subcodes of affine Reed-Muller codes are known for any number of variables [10, Thm. 11], and for projective Reed-Muller codes we also know how to obtain such sets of polynomials in the case of projective Reed-Solomon codes [13] and in the case of projective Reed-Muller codes over the projective plane [14]. For $m > 2$, we can apply Corollary D.4.2 and Corollary D.4.4 recursively until we reach the known cases of $m = 1$ or $m = 2$.

Example D.4.5. Let $q^s = 9$, $d = 4$, $m = 2$, and let ξ be a primitive element of $\mathbb{F}_9$. We are going to obtain a set of polynomials such that its image by the evaluation map is a basis for $\mathrm{PRM}_d^\sigma(m)$. Using Corollary D.4.4, we need to compute a basis for $\mathrm{RM}_3^\sigma(2)$ and $\mathrm{PRM}_4^\sigma(1)$. In the following we adopt the notation from [10] and [13] for denoting the polynomials we are going to use. The notation itself is not relevant for this example and we just use it to denote each polynomial. From [10, Thm. 11], we obtain that the image by the evaluation map over $\mathbb{F}_9^2$ of the following polynomials is a basis for $\mathrm{RM}_3^\sigma(2)$:

$$\mathcal{T}_{(0,0)}(1) = 1,\ \mathcal{T}_{(1,0)}(x_1) = x_1 + x_1^3,\ \mathcal{T}_{(1,0)}(\xi x_1) = \xi x_1 + \xi^3 x_1^3,$$
$$\mathcal{T}_{(0,1)}(x_2) = x_2 + x_2^3,\ \mathcal{T}_{(0,1)}(\xi x_2) = \xi x_2 + \xi^3 x_2^3.$$

From [13, Ex. 3.6], the image by the evaluation map over P^1 of the polynomials

$$\mathcal{T}_0^h(x_2^0) = x_1^4, \mathcal{T}_3^h(x_2^3) = x_1^3 x_2 + x_1 x_2^3, \mathcal{T}_3^h(\xi x_2^3) = \xi^3 x_1^3 x_2 + \xi x_1 x_2^3, \mathcal{T}_4^h(x_2^4) = x_2^4,$$

forms a basis for $\mathrm{PRM}_4^\sigma(1)$. By Corollary D.4.4, the image by the evaluation map over P^2 of the following set of polynomials is a basis for $\mathrm{PRM}_4^\sigma(2)$:

$$\{x_0^4, x_0^3 x_1 + x_0 x_1^3, \xi x_0^3 x_1 + \xi^3 x_0 x_1^3, x_0^3 x_2 + x_0 x_2^3, \xi x_0^3 x_2 + \xi^3 x_0 x_2^3\} \cup$$
$$\{x_1^4, x_1^3 x_2 + x_1 x_2^3, \xi^3 x_1^3 x_2 + \xi x_1 x_2^3, x_2^4\}.$$

We also obtain $\dim \mathrm{PRM}_4^\sigma(2) = 9$, which can also be obtained directly from Corollary D.4.2 because, as we have seen above, $\dim \mathrm{RM}_3^\sigma(2) = 5$ and $\dim \mathrm{PRM}_4^\sigma(1) = 4$.

As the dual of a projective Reed-Muller codes is another projective Reed-Muller code for $d \not\equiv 0 \bmod q^s - 1$ (by Theorem D.2.2), the recursive construction from Theorem D.3.1 can be used for the dual codes, except for the case $d \equiv 0 \bmod q^s - 1$. However, it is not true in general that $\mathrm{PRM}_d^{\sigma,\perp}(m) := (\mathrm{PRM}_d^\sigma(m))^\perp$ is equal to $\mathrm{PRM}_d^{\perp,\sigma}(m) := (\mathrm{PRM}_d^\perp(m))^\sigma$. Therefore, the construction from Corollary D.4.2 does not apply to the dual code of the subfield subcode of a projective Reed-Muller code. Nevertheless, in the next result we show that the dual codes can also be obtained from a similar recursive construction.

Proposition D.4.6. *Let $\xi \in \mathbb{F}_{q^s}$ be a primitive element. Let $m > 1$ and let $d_\lambda = \lambda \frac{q^s - 1}{q - 1}$ for some $\lambda \in \{1, 2, \ldots, m(q-1)\}$. Then we have*

$$\mathrm{PRM}_{d_\lambda}^{\sigma,\perp}(m) = \{(u^t, v^t - u_{\xi,d}^t), u^t \in \mathrm{RM}_{d_\lambda - 1}^{\sigma,\perp}(m), v^t \in \mathrm{PRM}_{d_\lambda}^{\sigma,\perp}(m-1)\},$$

where, taking into account the decomposition (D.3.1), if $u^t = (u_0^t, u_1^t, \ldots, u_{q^s-2}^t, u_{q^s-1}^t)$, with $u_0^t, \ldots, u_{q^s-2}^t \in \mathbb{F}_q^{p_{m-1}}$ and $u_{q^s-1}^t \in \mathbb{F}_q$, then

$$u_{\xi,d}^t := u_0^t + \xi^d u_1^t + \cdots + \xi^{(q^s-2)d} u_{q^s-2}^t = \sum_{i=0}^{q^s-2} \xi^{i \cdot d} u_i^t.$$

Proof. The vector space $\{(u^t, v^t - u^t_{\xi,d}), u^t \in \mathrm{RM}^{\sigma,\perp}_{d_\lambda-1}(m), v^t \in \mathrm{PRM}^{\sigma,\perp}_{d_\lambda}(m-1)\}$ has dimension $\dim \mathrm{RM}^{\sigma,\perp}_{d_\lambda-1}(m) + \dim \mathrm{PRM}^{\sigma,\perp}_{d_\lambda}(m-1)$, which is the dimension of $\mathrm{PRM}^{\sigma,\perp}_{d_\lambda}(m)$ according to Corollary D.4.2. Therefore, if we consider $u \in \mathrm{RM}^{\sigma}_{d_\lambda-1}(m)$, $v \in \mathrm{PRM}^{\sigma}_{d_\lambda}(m-1)$, $u^t \in \mathrm{RM}^{\sigma,\perp}_{d_\lambda-1}(m)$ and $v^t \in \mathrm{PRM}^{\sigma,\perp}_{d_\lambda}(m-1)$, by Corollary D.4.2 we just need to verify that

$$(u + v_{\xi,d}, v) \cdot (u^t, v^t - u^t_{\xi,d}) = v_{\xi,d} \cdot u^t - v \cdot u^t_\xi = 0.$$

By considering the decomposition (D.3.1), we can divide the vector u^t as in the statement of this result, and the previous expression can be written as

$$v_{\xi,d} \cdot u^t - v \cdot u^t_\xi = v \cdot u^t_0 + \xi^d v \cdot u^t_1 + \cdots + \xi^{(q^s-2)d} v \cdot u^t_{q^s-2} - v \cdot (u^t_0 + \xi^d u^t_1 + \cdots + \xi^{(q^s-2)d} u^t_{q^s-2}),$$

which is equal to 0. □

As with the recursive construction from Corollary D.4.2, the previous result can be used recursively because we know bases for $\mathrm{RM}^{\sigma,\perp}_{d_\lambda-1}(m)$ (for example, see [12]), and also for $\mathrm{PRM}^{\sigma,\perp}_{d_\lambda}(m)$, for $m = 1$ and $m = 2$, see [13, 14].

D.4.1 Examples

In this subsection we show that we can obtain good parameters with the subfield subcodes of projective Reed-Muller codes appearing in Corollary D.4.2 and Proposition D.4.6. For $m = 2$, the codes arising from Corollary D.4.2 are a particular case of the codes studied in [14]. However, for the degrees considered in Corollary D.4.2 we have an easier construction, and we show in Table D.1 that many of the codes with good parameters from [14] correspond precisely to the codes from Corollary D.4.2 or their duals from Proposition D.4.6. For the minimum distance of the codes from Corollary D.4.2 we can use the bound $d_1(\mathrm{PRM}^{\sigma}_d(m)) \geq d_1(\mathrm{PRM}_d(m))$, and for the duals we can compute the minimum distance with Magma [7]. All codes presented in Table D.1 exceed the Gilbert-Varshamov bound, and some of them have the best known parameters according to codetables [15], as stated in [14].

Table D.1: Codes with good parameters appearing in [14] that can be obtained from Corollary D.4.2 or Proposition D.4.6.

q	s	m	λ	Result	n	k	$d_1(C) \geq$
2	2	2	1	D.4.2	21	9	8
2	2	2	1	D.4.6	21	12	5
2	2	3	1	D.4.2	85	16	32
2	2	3	2	D.4.6	85	25	21
2	2	3	2	D.4.2	85	60	8
2	2	3	1	D.4.6	85	69	5
3	9	2	1	D.4.2	91	9	54
3	9	2	1	D.4.6	91	82	4
4	2	2	1	D.4.2	273	9	192
5	2	2	1	D.4.2	651	9	500
7	2	2	1	D.4.2	2451	9	2058

Furthermore, as the recursive approach from this work allows us to work easily with $m > 2$, we can also provide examples of good parameters which do not appear in [14]. As these codes are very long when we increase q^s, we only provide a few examples that still have moderate lengths. For the extension $\mathbb{F}_4 \supset \mathbb{F}_2$ and $m = 4$, for $\lambda = 1, 2$, from Corollary D.4.2 we obtain the codes $[341, 25, 128]_2$ and $[341, 295, 8]_2$, respectively, which surpass the Gilbert-Varshamov bound. The dual of the code with parameters $[341, 25, 128]_2$ has parameters $[341, 316, 5]_2$, which also exceed the Gilbert-Varshamov bound.

For the extension $\mathbb{F}_9 \supset \mathbb{F}_3$ and $m = 3$, we can consider $\lambda = 1$ in Corollary D.4.2, which gives a code with parameters $[820, 16, 486]_3$. Its dual has parameters $[820, 804, 4]_3$, and both of them surpass the Gilbert-Varshamov bound. We also note that, as we claimed in the introduction, by considering subfield subcodes we are able to obtain long codes with good parameters over a small finite field.

D.5 A bound for the generalized Hamming weights of projective Reed-Muller codes

In this section we provide a lower bound for the generalized Hamming weights of any projective Reed-Muller code. Let $C \subset \mathbb{F}_{q^s}^n$ be a linear code and $D \subset C$. The support of D, denoted by $\mathrm{supp}(D)$, is defined as

$$\mathrm{supp}(D) := \{i \mid \exists\ c = (c_1, \ldots, c_n) \in D,\ c_i \neq 0\}.$$

If D is a linear subspace contained in C, then we say that it is a subcode of C. The rth generalized Hamming weight of C, denoted by $d_r(C)$, is defined as

$$d_r(C) = \min\{|\mathrm{supp}(D)| \mid D \text{ is a subcode of } C \text{ with } \dim D = r\}.$$

Remark D.5.1. Given a basis $B = \{b_1, \ldots, b_k\}$ for a subcode D, we have that

$$\mathrm{supp}(D) = \bigcup_{i=1}^{k} \mathrm{supp}(b_i).$$

The generalized Hamming weights satisfy a Singleton-type bound and they are monotonous, as it is shown in the following results from [21].

Theorem D.5.2 (Monotonicity)**.** *For an $[n, k]$ linear code C with $k > 0$ we have*

$$1 \leq d_1(C) < d_2(C) < \cdots < d_k(C) \leq n.$$

Corollary D.5.3 (Generalized Singleton Bound)**.** *For an $[n, k]$ linear code C we have*

$$d_r(C) \leq n - k + r,\ 1 \leq r \leq k.$$

For an MDS code C with length n and dimension k, Theorem D.5.2 and Corollary D.5.3 imply that

$$d_r(C) = n - k + r,\ 1 \leq r \leq k.$$

For the affine case, the generalized Hamming weights of Reed-Muller codes were obtained in [16], where the authors give several ways to compute them. We present one of them now, which does not require additional machinery, see [16, Thm. 5.10]. Let $Q = \{0, \ldots, q^s - 1\}$. We consider the set Q^m with the lexicographic order. For $\beta \in Q^m$, we denote $\deg(\beta) = \sum_{i=1}^{m} \beta_i$.

Theorem D.5.4. *Let β be the rth element in Q^m in the lexicographic order with the property that*

$$\deg(\beta) > m(q^s - 1) - d - 1.$$

Then

$$d_r(\mathrm{RM}_d(m)) = \sum_{i=1}^{m} \beta_{m-i+1} q^{s(i-1)} + 1.$$

Our goal in this section is to provide a general lower bound for the generalized Hamming weights of any projective Reed-Muller code using the construction from Theorem D.3.1. We consider a degree d and $\xi \in \mathbb{F}_{q^s}$ a primitive element. Let $k_u = \dim(\mathrm{RM}_{d-1}(m))$ and $k_v = \dim(\mathrm{PRM}_d(m-1))$. We consider a basis $\{u^i\}_{i=1}^{k_u}$ for $\mathrm{RM}_{d-1}(m)$ and a basis $\{v^j\}_{j=1}^{k_v}$ for $\mathrm{PRM}_d(m-1)$. Then, by Theorem D.3.1, we have that $\mathcal{B} = \{u^i \times \{0\}^{p_{m-1}}\}_{i=1}^{k_u} \cup \{(v^j_{\xi,d}, v^j)\}_{j=1}^{k_v}$ is a basis for $\mathrm{PRM}_d(m)$. Given any subcode D of $\mathrm{PRM}_d(m)$ with $\dim D = r$, we consider a basis

$$\mathcal{B}_D = \{b_l, 1 \leq l \leq r\} := \left\{ \sum_{i=1}^{k_u} \lambda_{l,i} u^i \times \{0\}^{p_{m-1}} + \sum_{j=1}^{k_v} \mu_{l,j} (v^j_{\xi,d}, v^j), 1 \leq l \leq r \right\}.$$

Now we divide the vectors b_l into two parts, $b_l = (b_{l,1}, b_{l,2})$, where

$$b_{l,1} := \sum_{i=1}^{k_u} \lambda_{l,i} u^i + \sum_{j=1}^{k_v} \mu_{l,j} v^j_{\xi,d}\ ,\ b_{l,2} := \sum_{j=1}^{k_v} \mu_{l,j} v^j. \tag{D.5.1}$$

Remark D.5.5. By the definition, it is clear that $b_{l,2} \in \mathrm{PRM}_d(m-1)$. On the other hand, if $b_{l,2} = 0$, then $\mu_{l,j} = 0$ for all j and $b_{l,1} \in \mathrm{RM}_{d-1}(m)$. Moreover, in general we have $b_{l,1} \in \mathrm{RM}_d(m)$. This is because $b_{l,1}$ is the first part of b_l, which is a vector from $\mathrm{PRM}_d(m)$, i.e., is the evaluation of a homogeneous polynomial f of degree d. The evaluation of f in the first part of the decomposition (D.2.1) is the same as the evaluation of $g := f(1, x_1, \ldots, x_m)$ in $\mathbb{A}^m$, which belongs to $\mathrm{RM}_d(m)$.

If we consider the matrix G whose rows are given by the vectors in $\mathcal{B}_D$ we obtain

$$G = \begin{pmatrix} b_{1,1} & b_{1,2} \\ b_{2,1} & b_{2,2} \\ \vdots & \vdots \\ b_{r,1} & b_{r,2} \end{pmatrix}.$$

By performing row operations in G, and reordering the $b_{l,i}$ if necessary, we can assume that there is an integer $\alpha \leq r$ such that the set $\{b_{1,2}, \ldots, b_{\alpha,2}\}$ is linearly independent, and $b_{\alpha+1,2} = \cdots = b_{r,2} = 0$. Therefore, we have

$$G = \begin{pmatrix} b_{1,1} & b_{1,2} \\ \vdots & \vdots \\ b_{\alpha,1} & b_{\alpha,2} \\ b_{\alpha+1,1} & 0 \\ \vdots & \vdots \\ b_{r,1} & 0 \end{pmatrix}.$$

With the current ordering, note that the set $\{b_{\alpha+1,1}, \ldots, b_{r,1}\}$ is linearly independent (because $\mathcal{B}_D$ is a basis and G is a full rank matrix). Therefore, we can perform row operations in such a way that, after reordering the $b_{l,i}$ (if necessary), for $1 \leq l \leq \alpha$, we have an integer $\gamma \leq \alpha$ such that $b_{1,1} = \cdots = b_{\gamma,1} = 0$, and the set $\{b_{\gamma+1,1}, \ldots, b_{r,1}\}$ is linearly independent. Therefore, we can assume that G has the form

$$G = \begin{pmatrix} 0 & b_{1,2} \\ \vdots & \vdots \\ 0 & b_{\gamma,2} \\ b_{\gamma+1,1} & b_{\gamma+1,2} \\ \vdots & \vdots \\ b_{\alpha,1} & b_{\alpha,2} \\ b_{\alpha+1,1} & 0 \\ \vdots & \vdots \\ b_{r,1} & 0 \end{pmatrix} =: \begin{pmatrix} G_1 & G_2 \end{pmatrix}, \tag{D.5.2}$$

where $\{b_{1,2}, \ldots, b_{\alpha,2}\}$ and $\{b_{\gamma+1,1}, \ldots, b_{r,1}\}$ are linearly independent sets. Now we will give a lower bound for $|\mathrm{supp}(D)|$ for any subcode D of $\mathrm{PRM}_d(m)$ depending on the values of α and γ. Note that these values do not depend on the choice of $\mathcal{B}_D$. For technical reasons, in what follows we will understand that $d_0(C) = 0$ for a code $C \subset \mathbb{F}_{q^s}^n$.

Assuming that G has the form from (D.5.2), by using Remark D.5.5 we see that $\{b_{\alpha+1,1}, \ldots, b_{r,1}\}$ is contained in $\mathrm{RM}_{d-1}(m)$ and $\{b_{1,2}, \ldots, b_{\alpha,2}\}$ is contained in $\mathrm{PRM}_d(m-1)$. Both of these sets are linearly independent because of the assumptions on the form of G. Therefore, $r - \dim \mathrm{RM}_{d-1}(m) \leq \alpha \leq \dim \mathrm{PRM}_d(m-1)$ (we also have the obvious condition $\alpha \leq r$).

In order to bound $|\mathrm{supp}(D)|$, we note that $\mathrm{supp}(D)$ is the union of the supports of b_l, $1 \leq l \leq r$, by Remark D.5.1. Therefore, it is enough to study the union of the supports of the rows of G. Moreover, we can study the union of the support of the $b_{i,1}$ and $b_{j,2}$, $1 \leq i, j \leq r$, separately, which corresponds to studying the union of the supports of the rows of G_1 and G_2, which we denote by $\mathrm{supp}(G_1)$ and $\mathrm{supp}(G_2)$, respectively.

For G_1, by considering the last $r-\alpha$ rows it is clear that $|\mathrm{supp}(G_1)| \geq d_{r-\alpha}(\mathrm{RM}_{d-1}(m))$ using Remark D.5.5. Another possible bound is $|\mathrm{supp}(G_1)| \geq d_{r-\gamma}(\mathrm{RM}_d(m))$, which is obtained by considering all the rows of G_1 and Remark D.5.5. Therefore,

$$|\mathrm{supp}(G_1)| \geq \max(d_{r-\alpha}(\mathrm{RM}_{d-1}(m)), d_{r-\gamma}(\mathrm{RM}_d(m))).$$

For G_2, using Remark D.5.5 we have $|\mathrm{supp}(G_2)| \geq d_\alpha(\mathrm{PRM}_d(m-1))$. This bound can be improved by studying the first γ rows of G. This is because in order to have $b_{l,1} = 0$, by Theorem D.3.1 we also must have $b_{l,1} = u + v_{\xi,d} = 0$ for some $u \in \mathrm{RM}_{d-1}(m)$, $v \in \mathrm{PRM}_d(m-1)$. The vector u is the evaluation of a polynomial f of degree at most $d-1$ in $\mathbb{A}^m$, and $v_{\xi,d}$ is the evaluation of a homogeneous polynomial g of degree d in $\mathbb{A}^m$. We have the isomorphism given by the evaluation over the affine space

$$\mathbb{F}_{q^s}[x_1, \ldots, x_m]/\langle x_1^{q^s} - x_1, \ldots, x_m^{q^s} - x_m \rangle \cong \mathbb{A}^m.$$

As f and g have the opposite evaluation in $\mathbb{A}^m$, we must have $f \equiv -g \bmod \langle x_1^{q^s} - x_1, \ldots, x_m^{q^s} - x_m \rangle$. This implies that, if we consider $\overline{f}$ and $\overline{g}$ the polynomials obtained

by reducing all the exponents of the monomials of f and g, respectively, modulo q^s-1, then $\overline{f} = -\overline{g}$. As f is of degree at most $d-1$, $\overline{f}$ and $\overline{g}$ are of degree at most $d-1$. Taking into account that g is homogeneous of degree d, we deduce that all the exponents of the monomials of g can be reduced modulo q^s-1 (in order to have $\overline{g}$ of degree at most $d-1$), which implies that all the monomials from g reduce to monomials of degree at most $d-(q^s-1)$ in $\overline{g}$. Hence, g has the same evaluation as some homogeneous polynomial of degree $d-(q^s-1)$. Thus, $v \in \mathrm{PRM}_{d-(q^s-1)}(m-1)$. What we have obtained is that $b_{l,2} \in \mathrm{PRM}_{d-(q^s-1)}(m-1)$, $1 \leq l \leq \gamma$, and

$$|\mathrm{supp}(G_2)| \geq \max(d_\alpha(\mathrm{PRM}_d(m-1)), d_\gamma(\mathrm{PRM}_{d-(q^s-1)}(m-1))).$$

Therefore, for D we have

$$\begin{aligned} |\mathrm{supp}(D)| \geq B_{\alpha,\gamma} := &\max(d_{r-\gamma}(\mathrm{RM}_d(m)), d_{r-\alpha}(\mathrm{RM}_{d-1}(m))) \\ &+ \max(d_\alpha(\mathrm{PRM}_d(m-1)), d_\gamma(\mathrm{PRM}_{d-(q^s-1)}(m-1))). \end{aligned} \tag{D.5.3}$$

Note that, because of the previous reasoning and the form of G, we must have $r - \dim \mathrm{RM}_d(m) \leq \gamma \leq \dim \mathrm{PRM}_{d-(q^s-1)}(m-1)$ (besides $\gamma \leq \alpha$).

Remark D.5.6. The previous reasoning about $\mathrm{PRM}_{d-(q^s-1)}(m-1)$ implies that we can only have $\gamma > 0$ if $d \geq q^s$.

We summarize what we have obtained in the following result, where we understand that $\mathrm{PRM}_d = \{0\}$ for $d \leq 0$, and, as before, $d_0(C) = 0$ for a code $C \subset \mathbb{F}_{q^s}^n$.

Theorem D.5.7. *Let $1 \leq d \leq m(q^s-1)$ and $2 \leq r \leq \dim(\mathrm{PRM}_d(m))$. We consider*

$$Y = \left\{ (\alpha,\gamma) : \begin{array}{c} \max\{r - \dim \mathrm{RM}_{d-1}(m), 0\} \leq \alpha \leq \min\{\dim \mathrm{PRM}_d(m-1), r\} \\ \max\{r - \dim \mathrm{RM}_d(m), 0\} \leq \gamma \leq \min\{\dim \mathrm{PRM}_{d-(q^s-1)}(m-1), \alpha\} \end{array} \right\}.$$

Then we have

$$d_r(\mathrm{PRM}_d(m)) \geq \min_{(\alpha,\gamma)\in Y} B_{\alpha,\gamma},$$

where $B_{\alpha,\gamma}$ is defined in (D.5.3).

Proof. Given any subcode $D \subset \mathrm{PRM}_d(m)$ with $\dim D = r$, we can obtain a basis $\mathcal{B}_D$ for D such that when we consider the matrix G whose rows are the vectors of $\mathcal{B}_D$, this matrix is of the form from (D.5.2). Therefore, by the reasoning prior to this result, $|\mathrm{supp}(D)| \geq B_{\alpha,\gamma}$, for the integers α and γ deduced from G. By considering the bounds for the parameters α and γ obtained before, we obtain the set Y and we finish the proof. □

With the previous result we obtain lower bounds for all the generalized Hamming weights of projective Reed-Muller codes recursively. This is because we can apply the previous theorem recursively until we get to projective Reed-Solomon codes, in which case we have $d_r(\mathrm{PRM}_d(1)) = \max\{q^s - d + r, r\}$, for $1 \leq r \leq d+1$. With this starting point, and using Theorem D.5.4 for the generalized Hamming weights of affine Reed-Muller, we can compute the value of the previous bound for the generalized Hamming weight of any projective Reed-Muller code. This contrasts with the results from [3], where the authors are able to compute the generalized Hamming weights of projective Reed-Muller codes

in some cases and they also provide lower bounds, but only for $d < q^s$, while our bound works for any degree and any r.

We have checked by computer that the bound in Theorem D.5.7 is sharp for all the generalized Hamming weights with $m = 2, 3$, and $q^s = 2$; $m = 2$ and $q^s = 3$; and also for some particular degrees, such that $m = 3$, $q^s = 3$ and $d = 1$; and $m = 2$, $q^s = 4$ and $d = 1, 2$. As computing the generalized Hamming weights of a code is computationally intensive, we can only do it for smaller examples. It is therefore desirable to have some criterion to guarantee that the bound from Theorem D.5.7 is sharp in some cases, which is the purpose of the following result.

Lemma D.5.8. *Let* $1 \leq d \leq m(q^s - 1)$ *and* $2 \leq r \leq \max\{\dim \mathrm{RM}_{d-1}(m), \dim \mathrm{PRM}_d(m-1)\}$. *Then*

$$d_r(\mathrm{PRM}_d(m)) \leq \min\{d_r(\mathrm{RM}_{d-1}(m)), q^s \cdot d_r(\mathrm{PRM}_d(m-1))\},$$

where if $r > \dim \mathrm{RM}_{d-1}(m)$ *or* $r > \dim \mathrm{PRM}_d(m-1)$ *we do not consider the corresponding generalized Hamming weight in the minimum.*

Proof. We are going to find subcodes E' of $\mathrm{PRM}_d(m)$ such that $|\mathrm{supp}(E')| = d_r(\mathrm{RM}_{d-1}(m))$ or $|\mathrm{supp}(E')| = q^s \cdot d_r(\mathrm{PRM}_d(m-1))$. Assuming $r \leq \dim \mathrm{RM}_{d-1}(m)$, there is a subcode $E \subset \mathrm{RM}_{d-1}(m)$ with $\dim E = r$ and $|\mathrm{supp}(E)| = d_r(\mathrm{RM}_{d-1}(m))$. Then, the subcode $E' = E \times \{0\}^{p_{m-1}} \subset \mathrm{PRM}_d(m)$ verifies $|\mathrm{supp}(E')| = d_r(\mathrm{RM}_{d-1}(m))$.

If we assume that $r \leq \dim \mathrm{PRM}_d(m-1)$ instead, there is a subcode $E \subset \mathrm{PRM}_d(m-1)$ with $\dim E = r$, such that $|\mathrm{supp}(E)| = d_r(\mathrm{PRM}_d(m-1))$. The subcode

$$E' := \{(v_{\xi,d}, v), v \in E\} \subset \mathrm{PRM}_d(m)$$

verifies $|\mathrm{supp}(E')| = q^s \cdot d_r(\mathrm{PRM}_d(m-1))$. □

We can use Lemma D.5.8, together with Theorem D.5.2, in order to ensure that the bound from Theorem D.5.7 is sharp in many cases. We see this in Example D.5.9 and in Subsection D.5.3, where we show the tables that we obtain using our results for the generalized Hamming weights of projective Reed-Muller codes for several finite fields. Notwithstanding the foregoing, as we will see in Example D.5.10, we can also find particular cases in which the bound is not sharp.

Example D.5.9. Let $q^s = 4$, $d = 5$, $m = 2$ and $r = 2$. In this example we are going to compute the bound from Theorem D.5.7 for $d_2(\mathrm{PRM}_5(2))$. From Theorem D.2.3 we can obtain $\dim \mathrm{RM}_4(2) = 13$ and $\dim \mathrm{RM}_5(2) = 15$. For $m = 2$, $\mathrm{PRM}_d(m-1)$ is a projective Reed-Solomon code, and for $d = 5 > 4 = q^s$ we have $\mathrm{PRM}_5(1) = \mathbb{F}_{q^s}^{q^s+1}$, which implies $\dim \mathrm{PRM}_5(1) = q^s + 1$. Moreover, for $d - (q^s - 1) = 2$, we have $\dim \mathrm{PRM}_2(1) = 3$. Therefore, we obtain

$$Y = \left\{(\alpha, \gamma) : \begin{array}{l} 0 \leq \alpha \leq 2 \\ 0 \leq \gamma \leq \alpha \end{array}\right\} = \{(0,0), (1,0), (1,1), (2,0), (2,1), (2,2)\}.$$

Now we have to compute $\min_{(\alpha,\gamma)\in Y} B_{\alpha,\gamma}$. In order to do it, we need to obtain the generalized Hamming weights for affine Reed-Muller codes and projective Reed-Solomon codes. For projective Reed-Solomon codes, we have already stated that we have $d_r(\mathrm{PRM}_d(1)) =$

r	1	2
$d_r(\mathrm{RM}_5(2))$	2	3
$d_r(\mathrm{RM}_4(2))$	3	4

$\max\{q^s - d + r, r\}$, and for affine Reed-Muller codes we can use Theorem D.5.4 in order to obtain

With all of this we can compute all the values $B_{\alpha,\gamma}$, for $(\alpha,\gamma) \in Y$:

$$
\begin{aligned}
&B_{0,0} = d_2(\mathrm{RM}_4(2)) = 4,\\
&B_{1,0} = \max\{d_2(\mathrm{RM}_5(2)), d_1(\mathrm{RM}_4(2))\} + d_1(\mathrm{PRM}_5(1)) = \max\{3,3\} + 1 = 4,\\
&B_{1,1} = \max\{d_1(\mathrm{RM}_5(2)), d_1(\mathrm{RM}_4(2))\} + \max\{d_1(\mathrm{PRM}_5(1)), d_1(\mathrm{PRM}_2(1))\} = 6,\\
&B_{2,0} = d_2(\mathrm{RM}_5(2)) + d_2(\mathrm{PRM}_5(1)) = 3 + 2 = 5,\\
&B_{2,1} = d_1(\mathrm{RM}_5(2)) + \max\{d_2(\mathrm{PRM}_5(1)), d_1(\mathrm{PRM}_2(1))\} = 2 + \max\{2,3\} = 5,\\
&B_{2,2} = \max\{d_2(\mathrm{PRM}_5(1)), d_2(\mathrm{PRM}_2(1))\} = \max\{2,4\} = 4.
\end{aligned}
$$

Therefore, we have obtained

$$d_r(\mathrm{PRM}_d(m)) \geq \min_{(\alpha,\gamma)\in Y} B_{\alpha,\gamma} = 4.$$

Moreover, as $\min_{(\alpha,\gamma)\in Y} B_{\alpha,\gamma} = B_{0,0} = d_r(\mathrm{RM}_{d-1}(2))$, by Lemma D.5.8 we know that we have the equality $d_r(\mathrm{PRM}_d(m)) = 4$.

Example D.5.10. In this example we show a particular case in which the bound from Theorem D.5.7 is not sharp. Let $q^s = 4$, $d = 3$, $m = 2$ and $r = 2$. Using Theorem D.2.3, we obtain $\dim \mathrm{RM}_2(2) = 6$ and $\dim \mathrm{RM}_3(2) = 10$. For $\mathrm{PRM}_d(1)$, we have that this code is a projective Reed-Solomon code, and therefore its dimension is $d + 1 = 4$ in this case. Thus,

$$Y = \left\{(\alpha,\gamma) : \begin{array}{c} 0 \leq \alpha \leq 2 \\ 0 \leq \gamma \leq 0 \end{array}\right\} = \{(0,0),(1,0),(2,0)\}.$$

Note that $\gamma = 0$ because $d < q^s$, see Remark D.5.6. With respect to the generalized Hamming weights of affine Reed-Muller codes, we can use Theorem D.5.4 to obtain:

r	1	2
$d_r(\mathrm{RM}_3(2))$	4	7
$d_r(\mathrm{RM}_2(2))$	8	11

Now we have all the values required in order to compute the bound from Theorem D.5.7:

$$
\begin{aligned}
&B_{0,0} = d_2(\mathrm{RM}_2(2)) = 11,\\
&B_{1,0} = \max\{d_2(\mathrm{RM}_3(2), d_1(\mathrm{RM}_2(2))\} + d_1(\mathrm{PRM}_1(1)) = \max\{7,8\} + 2 = 10,\\
&B_{2,0} = d_2(\mathrm{RM}_3(2) + d_2(\mathrm{PRM}_1(1)) = 7 + 3 = 10,
\end{aligned}
$$

where we have used that $d_r(\mathrm{PRM}_d(1)) = q^s - d + r$ for $d \leq q^s$. Therefore,

$$d_2(\mathrm{PRM}_3(2)) \geq \min_{(\alpha,\gamma)\in Y} B_{\alpha,\gamma} = \min\{11,10,10\} = 10.$$

However, according to [3, Ex 7.5], the true value is $d_2(\mathrm{PRM}_3(2)) = 11$ in this case.

Example D.5.11. We mainly use Lemma D.5.8 with the bound

$$d_r(\mathrm{PRM}_d(m)) \leq d_r(\mathrm{RM}_{d-1}(m)) = B_{0,0},$$

but the part

$$d_r(\mathrm{PRM}_d(m)) \leq q^s \cdot d_r(\mathrm{PRM}_d(m-1))$$

is also useful in some cases. For example, for $q^s = 3$, $d = 1$, $r = 2$, $m = 2$, one can check that $\min_{(\alpha,\gamma)\in Y} B_{\alpha,\gamma} = 12$. We cannot use the bound $d_r(\mathrm{PRM}_d(m)) \leq d_r(\mathrm{RM}_{d-1}(m))$ because $\dim \mathrm{RM}_0(2) = 1 < 2 = r$. However, we have $r = 2 = \dim \mathrm{PRM}_1(1)$, and $12 = q^s \cdot d_2(\mathrm{PRM}_1(1))$.

In the previous case, the bound was useful because we could not use $d_r(\mathrm{PRM}_d(m)) \leq d_r(\mathrm{RM}_{d-1}(m))$. Nevertheless, there are also cases in which the bound $d_r(\mathrm{PRM}_d(m)) \leq q^s \cdot d_r(\mathrm{PRM}_d(m-1))$ is better than the bound $d_r(\mathrm{PRM}_d(m)) \leq d_r(\mathrm{RM}_{d-1}(m))$. For instance, for $q^s = 3$, $d = 3$, $r = 2$, $m = 3$, we have $d_2(\mathrm{RM}_2(3)) = 15 > 12 = 3 \cdot d_2(\mathrm{PRM}_3(2))$. In fact, one can also check in this case that $\min_{(\alpha,\gamma)\in Y} B_{\alpha,\gamma} = 12$ and we can state that the bound from Theorem D.5.7 is sharp due to Lemma D.5.8.

D.5.1 A bound for the projective Reed-Muller codes over $\mathbb{P}^2$

Even though the bound from Theorem D.5.7 is not hard to obtain by computer in general, it can be obtained in more efficient ways in some particular cases. In this subsection, we are going to obtain the bound from Theorem D.5.7 in a more explicit way and requiring less values of $B_{\alpha,\gamma}$ in order to compute the minimum over Y, for the case $m = 2$.

Theorem D.5.12. *Let $1 \leq d \leq 2(q^s - 1)$, $2 \leq r \leq \dim(\mathrm{PRM}_d(2))$, and Y as in Theorem D.5.7.*

(a) If $d < q^s$, we consider α_0 the smallest integer such that $d_{r-\alpha_0}(\mathrm{RM}_{d-1}(2)) \leq d_r(\mathrm{RM}_d(2))$, $\mu_0 = \max\{\alpha_0, r - \dim \mathrm{RM}_{d-1}(2)\}$ and $\lambda = \min\{d+1, r\}$. Then

$$d_r(\mathrm{PRM}_d(2)) \geq \min_{(\alpha,\gamma)\in Y} B_{\alpha,\gamma} = \begin{cases} \min\{B_{0,0}, H_{\alpha_0,0}\} & \text{if } r \leq \dim \mathrm{RM}_{d-1}(2), \\ B_{\alpha_0,0} & \text{if } r > \dim \mathrm{RM}_{d-1}(2), \end{cases}$$

where $B_{0,0} = d_r(\mathrm{RM}_{d-1}(2))$ and

$$H_{\alpha_0,0} = \begin{cases} d_r(\mathrm{RM}_d(2)) + q^s - d + \mu_0 & \text{if } \alpha_0 \leq \lambda, \\ d_{r-\lambda}(\mathrm{RM}_{d-1}(2)) + q^s - d + \lambda & \text{if } \alpha_0 > \lambda. \end{cases}$$

(b) If $d \geq q^s$, we consider

$$E = \{\gamma \mid \max\{r - \dim \mathrm{RM}_d(2), 0\} \leq \gamma \leq \min\{d - q^s + 2, r\}\}.$$

Let $i \leq \alpha_i \leq r$ be the smallest integer such that $d_{r-\alpha_i}(\mathrm{RM}_{d-1}(2)) \leq d_{r-i}(\mathrm{RM}_d(2))$, for $i \in E$. We also consider $\mu_i = \max\{\alpha_i, r - \dim \mathrm{RM}_{d-1}(2)\}$ and $\lambda = \min\{q^s + 1, r\}$. Then

$$d_r(\mathrm{PRM}_d(2)) \geq \min_{(\alpha,\gamma)\in Y} B_{\alpha,\gamma} = \begin{cases} \min\{B_{0,0}, \min_{\gamma\in E}\{H_{\alpha_\gamma,\gamma}\}\} & \text{if } r \leq \dim \mathrm{RM}_{d-1}(2), \\ \min_{\gamma\in E}\{H_{\alpha_\gamma,\gamma}\} & \text{if } r > \dim \mathrm{RM}_{d-1}(2), \end{cases} \tag{D.5.4}$$

where $B_{0,0} = d_r(\mathrm{RM}_{d-1}(2))$ *and*

$$H_{\alpha_\gamma,\gamma} = \begin{cases} d_r(\mathrm{RM}_d(2)) + \mu_0 & \text{if } \gamma = 0, \alpha_\gamma \leq \lambda, \\ d_{r-\lambda}(\mathrm{RM}_{d-1}(2)) + \lambda & \text{if } \gamma = 0, \alpha_\gamma > \lambda, \\ d_{r-\gamma}(\mathrm{RM}_d(2)) + \max\{\mu_\gamma, 2q^s - d + \gamma - 1\} & \text{if } \gamma > 0, \alpha_\gamma \leq \lambda, \\ d_{r-\lambda}(\mathrm{RM}_{d-1}(2)) + \max\{\lambda, 2q^s - d + \gamma - 1\} & \text{if } \gamma > 0, \alpha_\gamma > \lambda. \end{cases} \tag{D.5.5}$$

Moreover, in both cases if $\min_{(\alpha,\gamma)\in Y} B_{\alpha,\gamma} = B_{0,0} = d_r(\mathrm{RM}_{d-1}(2))$ *or* $\min_{(\alpha,\gamma)\in Y} B_{\alpha,\gamma} = q^s \cdot \max\{q^s - d + r, r\}$*, for* $r \leq \dim \mathrm{RM}_{d-1}(2)$ *or* $r \leq \min\{d+1, q^s+1\}$*, respectively, then the bound is sharp.*

Proof. We are going to prove the statement for $d \geq q^s$ and $r \leq \dim \mathrm{RM}_{d-1}(2)$ because the rest of the cases are argued in the same way (for instance, the case $d < q^s$ is analogous to the case of $\gamma = 0$ with $d \geq q^s$, see Remark D.5.6). If we prove the equality in (D.5.4), the rest follows from Theorem D.5.7 and Lemma D.5.8.

For $d \geq q^s$, we can rewrite the set Y from Theorem D.5.7 for the case $m = 2$ in the following way:

$$Y = \left\{ (\alpha,\gamma) : \begin{array}{c} \max\{r - \dim \mathrm{RM}_{d-1}(2), \gamma\} \leq \alpha \leq \min\{q^s+1, r\} \\ \max\{r - \dim \mathrm{RM}_d(2), 0\} \leq \gamma \leq \min\{d - q^s + 2, r\} \end{array} \right\},$$

where we have used the expressions for the dimension of the corresponding projective Reed-Solomon codes and we have written the conditions for α in terms of γ. For each $\gamma \in E$ we consider

$$Y_\gamma = \{\alpha \mid (\alpha,\gamma) \in Y\}.$$

This set is nonempty for each $\gamma \in E$ because $\gamma \leq \min\{d - q^s + 2, r\} \leq \min\{q^s+1, r\}$, and we also have $r - \dim \mathrm{RM}_{d-1}(2) \leq \min\{q^s+1, r\}$ because of Corollary D.3.3. We have that $Y = \bigcup_{\gamma\in E} Y_\gamma$, and therefore

$$\min_{(\alpha,\gamma)\in Y} B_{\alpha,\gamma} = \min_{\gamma\in E}\{\min_{\alpha\in Y_\gamma} B_{\alpha,\gamma}\}.$$

For $\gamma \in E$ fixed, we are going to study now the behavior of $B_{\alpha,\gamma}$, as defined in (D.5.3), as a function of α. We first consider the case with $\gamma > 0$. As we are assuming $2(q^s-1) \geq d \geq q^s$, we have that $\mathrm{PRM}_d(1) = \mathbb{F}_{q^s}^{q^s+1}$. Therefore, for $\alpha \geq \gamma > 0$, we have

$$\max\{d_\alpha(\mathrm{PRM}_d(1)), d_\gamma(\mathrm{PRM}_{d-(q^s-1)}(1))\} = \max\{\alpha, 2q^s - d + \gamma - 1\}.$$

For $\gamma > 0$ fixed, $\max\{\alpha, 2q^s - d + \gamma - 1\}$ is a nondecreasing function of α. For $1 \leq \alpha < \alpha_\gamma$ we have that

$$\max\{d_{r-\gamma}(\mathrm{RM}_d(2)), d_{r-\alpha}(\mathrm{RM}_{d-1}(2))\} = d_{r-\alpha}(\mathrm{RM}_{d-1}(2)).$$

Using Theorem D.5.2, we see that this value decreases in at least one unit when we increase α in one unit, while $\max\{\alpha, 2q^s - d + \gamma - 1\}$ is going to increase by at most one unit. Therefore, $B_{\alpha,\gamma}$ is a nonincreasing function of α, for $1 \leq \alpha < \alpha_\gamma$.

For $\alpha \geq \alpha_\gamma$, we have

$$\max\{d_{r-\gamma}(\mathrm{RM}_d(2)), d_{r-\alpha}(\mathrm{RM}_{d-1}(2))\} = d_{r-\gamma}(\mathrm{RM}_d(2)),$$

which is constant for a fixed γ. As $\max\{\alpha, 2q^s - d + \gamma - 1\}$ is nondecreasing, we obtain that $B_{\alpha,\gamma}$ is a nondecreasing function of α, for $\alpha_\gamma \leq \alpha \leq r$.

Therefore, we know the behavior of $B_{\alpha,\gamma}$ and we can obtain $\min_{\alpha \in Y_\gamma} B_{\alpha,\gamma}$. Indeed, for $1 \leq \alpha < \alpha_\gamma$, $B_{\alpha,\gamma}$ is nonincreasing, and therefore, $\min_{\alpha \in Y_\gamma, \alpha < \alpha_\gamma} B_{\alpha,\gamma}$ is attained at the largest value of $\alpha \in Y_\gamma$ such that $\alpha < \alpha_\gamma$ (if any). And, as $B_{\alpha,\gamma}$ is nondecreasing for $\alpha_\gamma \leq \alpha \leq r$, we have that $\min_{\alpha \in Y_\gamma, \alpha \geq \alpha_\gamma} B_{\alpha,\gamma}$ is attained at the lowest value of $\alpha \in Y_\gamma$ such that $\alpha \geq \alpha_\gamma$. In order to obtain $\min_{\alpha \in Y_\gamma} B_{\alpha,\gamma}$, we just need to consider the minimum between the minimums in the case $1 \leq \alpha < \alpha_\gamma$ and $\alpha_\gamma \leq \alpha \leq r$. We have two cases:

(a) If $\alpha_\gamma \leq \lambda$: by definition, $\alpha_\gamma \geq \gamma$. Therefore, we have $\alpha_\gamma \in Y_\gamma$ if and only if $r - \dim \mathrm{RM}_{d-1}(2) \leq \alpha_\gamma$, which happens if and only if $\mu_\gamma = \alpha_\gamma$. If $\alpha_\gamma > r - \dim \mathrm{RM}_{d-1}(2)$, all the values of Y_γ are larger than α_γ, i.e., we are in the nondecreasing part of $B_{\alpha,\gamma}$, and the minimum of $B_{\alpha,\gamma}$ over Y_γ is thus obtained at the lowest value of Y_γ, which is precisely $r - \dim \mathrm{RM}_{d-1}(2) = \mu_\gamma$ in this case. By the definition of α_γ, we have

$$B_{\mu_\gamma,\gamma} = d_{r-\gamma}(\mathrm{RM}_d(2)) + \max\{\mu_\gamma, 2q^s - d + \gamma - 1\}.$$

On the other hand, if $\alpha_\gamma \leq r - \dim \mathrm{RM}_{d-1}(2)$, i.e., $\alpha_\gamma = \mu_\gamma$, then the minimum in the nondecreasing part is $B_{\alpha_\gamma,\gamma} = B_{\mu_\gamma,\gamma}$ as above. If $\alpha_\gamma - 1 \notin Y_\gamma$, this is the minimum over Y_γ. If $\alpha_\gamma - 1 \in Y_\gamma$, we have to also consider the minimum over the nonincreasing part, which, taking into account the definition of α_γ, would be

$$B_{\alpha_\gamma - 1,\gamma} = d_{r-(\alpha_\gamma - 1)}(\mathrm{RM}_{d-1}(2)) + \max\{\alpha_\gamma - 1, 2q^s - d + \gamma - 1\}.$$

If we compute the difference we obtain

$$B_{\alpha_\gamma - 1,\gamma} - B_{\alpha_\gamma,\gamma} \geq d_{r-(\alpha_\gamma - 1)}(\mathrm{RM}_{d-1}(2)) - d_{r-\gamma}(\mathrm{RM}_d(2)) - 1 \geq 0$$

because of the definition of α_γ. Hence, in this case we also obtain $\min_{\alpha \in Y_\gamma} B_{\alpha,\gamma} = B_{\mu_\gamma,\gamma}$.

(b) If $\alpha_\gamma > \lambda$: we have that all the values of Y_γ are below α_γ, i.e., we are in the nonincreasing part of $B_{\alpha,\gamma}$. The minimum is thus obtained at the maximum value in Y_γ, which is λ, and by the definition of α_γ we have

$$B_{\lambda,\gamma} = d_{r-\lambda}(\mathrm{RM}_{d-1}(2)) + \max\{\lambda, 2q^s - d + \gamma - 1\}.$$

For the case with $\gamma = 0$, we have $\max\{d_\alpha(\mathrm{PRM}_d(1)), d_\gamma(\mathrm{PRM}_{d-(q^s-1)}(1))\} = \alpha$. The previous argument also applies in this case for the $\alpha \in Y_0$ with $\alpha > 0$ because this does not change the behaviour of $B_{\alpha,\gamma}$ (it only changes the exact expression of $B_{\alpha,\gamma}$, as seen in the statement). Therefore the minimum of $B_{\alpha,\gamma}$ in $Y_0 \setminus \{0\}$ is either $B_{\mu_\gamma,\gamma}$ or $B_{\lambda,\gamma}$ as before. If $0 \in Y_0$, which happens if and only if $r \leq \dim \mathrm{RM}_{d-1}(2)$, we also have to take into account for the minimum the bound $B_{0,0} = d_r(\mathrm{RM}_{d-1}(2))$. We complete the proof by noting that $H_{\alpha_\gamma,\gamma}$ is equal to $B_{\mu_\gamma,\gamma}$ or $B_{\lambda,\gamma}$, depending on where the minimum is attained in each case. □

One can also express the previous result in a more explicit way by taking into account that

$$\dim \mathrm{RM}_d(2) = \begin{cases} \binom{d+2}{2} & \text{if } d < q^s, \\ \binom{d+2}{2} - 2\binom{d-q^s+2}{2} & \text{if } q^s \leq d \leq 2(q^s - 1), \end{cases} \tag{D.5.6}$$

which can be proven from Theorem D.2.3.

Although Theorem D.5.12 looks more involved than Theorem D.5.7, it can greatly simplify the procedure of computing the bound from Theorem D.5.7 for the case $m = 2$, as we show in the next example.

Example D.5.13. Let $q^s = 4$, $d = 5$, $m = 2$ and $r = 5$. We are going to use Theorem D.5.12 in order to obtain a bound for $d_4(\mathrm{PRM}_5(2))$. As we have $d \leq q^s$, we compute $\dim \mathrm{RM}_5(2) = 15$ with (D.5.6) and we obtain

$$E = \{\gamma \mid 0 \leq \gamma \leq 3\}.$$

Using Theorem D.5.4, we can compute

r	1	2	3	4	5
$d_r(\mathrm{RM}_5(2))$	2	3	4	5	6
$d_r(\mathrm{RM}_4(2))$	3	4	6	7	8

From this table we obtain $\alpha_0 = 2$, $\alpha_1 = \alpha_2 = 3$ and $\alpha_3 = 4$. For example, we check that $d_{5-3}(\mathrm{RM}_4(2)) = 4 \leq 5 = d_{5-2}(\mathrm{RM}_{5-1}(2))$, but $d_{5-2}(\mathrm{RM}_4(2)) = 6 > 5 = d_{5-2}(\mathrm{RM}_{5-1}(2))$, which implies $\alpha_2 = 3$. Using (D.5.6) again, we can compute $\dim \mathrm{RM}_4(2) = 13$, which implies that $r - \dim \mathrm{RM}_4(2) < 0$ and $\mu_i = \alpha_i$ for $i = 0, 1, 2, 3$. We also have $\lambda = \min\{q^s + 1, r\} = 5$. Thus, $\alpha_i < \lambda$ for $i = 0, 1, 2, 3$. The only thing left to do is to compute $B_{0,0}$ and $H_{\alpha_\gamma,\gamma}$, for $\gamma \in E$. We obtain

$$\begin{aligned}
B_{0,0} &= d_5(\mathrm{RM}_4(2)) = 8,\\
H_{2,0} &= d_5(\mathrm{RM}_5(2)) + \mu_0 = 6 + 2 = 8,\\
H_{3,1} &= d_4(\mathrm{RM}_5(2)) + \max\{\mu_1, 2q^s - d + 1 - 1\} = 5 + \max\{3, 3\} = 8,\\
H_{3,2} &= d_3(\mathrm{RM}_5(2)) + \max\{\mu_2, 2q^s - d + 2 - 1\} = 4 + \max\{3, 4\} = 8,\\
H_{4,3} &= d_2(\mathrm{RM}_5(2)) + \max\{\mu_3, 2q^s - d + 3 - 1\} = 3 + \max\{4, 5\} = 8.
\end{aligned}$$

The minimum of these values is 8, and we have $d_5(\mathrm{PRM}_5(2)) \geq 8$. Furthermore, as the minimum is equal to $B_{0,0}$, by Theorem D.5.12 (or Lemma D.5.8) we have the equality $d_5(\mathrm{PRM}_5(2)) = 8$.

Note that if we want to use Theorem D.5.7 in order to obtain the bound for $d_5(\mathrm{PRM}_5(2))$, we would have to consider the minimum of $|Y|$ terms. In this case, we have

$$Y = \left\{(\alpha, \gamma) : \begin{array}{c} \gamma \leq \alpha \leq \min\{q^s + 1, r\} = 5 \\ 0 \leq \gamma \leq \min\{d - q^s + 2, r\} = 3 \end{array}\right\}.$$

Thus, using Theorem D.5.7 we would have to consider the minimum of $|Y| = 18$ terms, while using Theorem D.5.12 we only needed 5.

D.5.2 A bound for the generalized Hamming weights of the subfield subcodes of projective Reed-Muller codes

The subfield subcodes of Section D.4 are subcodes of projective Reed-Muller codes and therefore the generalized Hamming weights of projective Reed-Muller codes give lower

bounds for the generalized Hamming weights of the corresponding subfield subcodes. However, as the dimension of the subfield subcode is usually much smaller than the dimension of the original code, this bound is not sharp for most of the generalized Hamming weights. Nevertheless, Theorem D.5.7 and Lemma D.5.8 can be adapted for the subfield subcodes as well.

Corollary D.5.14. *Let $\xi \in \mathbb{F}_{q^s}$ be a primitive element and $m > 1$. Let $d_\lambda = \lambda\frac{q^s-1}{q-1}$ for some $\lambda \in \{1, 2, \ldots, m(q-1)\}$ and $2 \leq r \leq \dim(\mathrm{PRM}_d^\sigma(m))$. We consider*

$$Y^\sigma = \left\{(\alpha,\gamma) : \begin{array}{c} \max\{r - \dim \mathrm{RM}^\sigma_{d_\lambda-1}(m), 0\} \leq \alpha \leq \min\{\dim \mathrm{PRM}^\sigma_{d_\lambda}(m-1), r\} \\ \max\{r - \dim \mathrm{RM}^\sigma_{d_\lambda}(m), 0\} \leq \gamma \leq \min\{\dim \mathrm{PRM}^\sigma_{d_\lambda-(q^s-1)}(m-1), \alpha\} \end{array} \right\}.$$

Then we have

$$d_r(\mathrm{PRM}^\sigma_{d_\lambda}(m)) \geq \min_{(\alpha,\gamma)\in Y^\sigma} B^\sigma_{\alpha,\gamma},$$

where

$$B^\sigma_{\alpha,\gamma} := \max(d_{r-\gamma}(\mathrm{RM}^\sigma_{d_\lambda}(m)), d_{r-\alpha}(\mathrm{RM}^\sigma_{d_\lambda-1}(m))) + \max(d_\alpha(\mathrm{PRM}^\sigma_{d_\lambda}(m-1)), d_\gamma(\mathrm{PRM}^\sigma_{d_\lambda-(q^s-1)}(m-1))).$$

Proof. We consider the recursive construction from Corollary D.4.2, and we apply an analogous reasoning to the one above Theorem D.5.7. □

Corollary D.5.15. *Let $\xi \in \mathbb{F}_{q^s}$ be a primitive element and $m > 1$. Let $d_\lambda = \lambda\frac{q^s-1}{q-1}$ for some $\lambda \in \{1, 2, \ldots, m(q-1)\}$ and $2 \leq r \leq \max\{\dim \mathrm{RM}^\sigma_{d_\lambda-1}(m), \dim \mathrm{PRM}^\sigma_{d_\lambda}(m-1)\}$. Then*

$$d_r(\mathrm{PRM}^\sigma_{d_\lambda}(m)) \leq \min\{d_r(\mathrm{RM}^\sigma_{d_\lambda-1}(m)), q^s \cdot d_r(\mathrm{PRM}^\sigma_{d_\lambda}(m-1))\},$$

where if $r > \dim \mathrm{RM}^\sigma_{d_\lambda-1}(m))$ or $r > \dim \mathrm{PRM}^\sigma_{d_\lambda}(m-1)$ we do not consider the corresponding generalized Hamming weight in the minimum.

Proof. We consider the recursive construction from Corollary D.4.2 and argue as in the proof of Lemma D.5.8. □

With respect to the values that appear in these results, we have formulas for the dimension of the subfield subcodes of affine Reed-Muller codes [10, Thm. 11] and for the subfield subcodes of projective Reed-Muller codes over $\mathbb{P}^2$ [14, Cor. 3.41]. However, we do not have explicit results about the generalized Hamming weights of the subfield subcodes in the affine case or the projective case, besides the bounds given by the generalized Hamming weights of the affine or projective Reed-Muller codes. Therefore, although Corollary D.5.14 and Corollary D.5.15 are of theoretical interest, their practical utility is more limited than that of Theorem D.5.7 and Lemma D.5.8.

D.5.3 Examples

In this subsection we provide tables showing examples of how one can use the results in Section D.5 to determine the generalized Hamming weights of some projective Reed-Muller codes. In order to use the bound from Theorem D.5.7, we are going to use the true values for the minimum distances of projective Reed-Muller codes from Theorem D.2.1. We are going to use Theorem D.5.7 in order to provide a lower bound, and we can

use Lemma D.5.8 in order to give an upper bound in some cases. Moreover, if we know the true value of a generalized Hamming weight $d_r(\mathrm{PRM}_d(m))$, for $r' \leq r$ we know that $d_{r'}(\mathrm{PRM}_d(m)) \leq d_r(\mathrm{PRM}_d(m)) - (r - r')$ due to the monotonicity from Theorem D.5.2, which provides another upper bound. With this we can obtain the tables that we present below. Note that we are only using the bounds that we have just stated, we are not considering the values obtained in other papers such as [3]. For instance, by considering the values given in Example D.5.10, we see that $d_2(\mathrm{PRM}_3(2)) = 11$ for $q^s = 4$. Looking at Table D.4, we see that this also implies that $d_3(\mathrm{PRM}_3(2)) = 12$ by Theorem D.5.2, and we would therefore obtain all the generalized Hamming weights of $\mathrm{PRM}_3(2)$ for $q^s = 4$. Nevertheless, as it is seen in the tables, we can still obtain many of the true values of the generalized Hamming weights for projective Reed-Muller codes.

With respect to the notation, we will use dots when the generalized Hamming weights grow by one unit when increasing r. Unless stated otherwise, the value of the bound from Theorem D.5.7 coincides with the value of the generalized Hamming weight that appears in the table. When that does not happen (or if we do not know the true value), we will write the lower bound from Theorem D.5.7 and the best of the upper bounds that we have discussed above. We note that, for all the values that we omit by using dots, the bound from Theorem D.5.7 is sharp.

As we stated previously, for $q^s = 2$ we have checked by computer that we obtain the true values of $d_r(\mathrm{PRM}_d(m))$ for $m = 2, 3$. However, this case is not that important in the projective setting because, for $q^s = 2$, we have $\mathbb{P}^m = \mathbb{A}^{m+1} \setminus \{(0, \ldots, 0)\}$. Therefore, the projective Reed-Muller codes over $\mathbb{F}_2$ in $\mathbb{P}^m$ are equal to the shortening of affine Reed-Muller codes over in $m + 1$ variables over $\mathbb{F}_2$ at the point $(0, \ldots, 0)$.

Table D.2: Generalized Hamming weights for $q^s = 3$, $m = 2$.

$d\backslash r$	2	3	4	5	6	7	8	9	10	11	12	13
1	12	13										
2	8	9	11	12	13							
3	4-5	6	7	8	9	10	11	12	13			
4	3	4	5	6	7	8	9	10	11	12	13	

Table D.3: Generalized Hamming weights for $q^s = 3$, $m = 3$.

$d\backslash r$	2	3	4	5	6	7	8	9	10	11	12	13	$\cdots$	20
1	36	39	40											
2	23-24	26	27	32-35	35-36	36-37	38	39	40					
3	12	13-17	18	21	22-23	24	25	26	27	30-31	31-32	33	$\cdots$	40

$d\backslash r$	2	3	4	5	6	7	8	9	10	11	$\cdots$	17	18	$\cdots$	29
4	8	9	11-12	12-14	13-15	15-16	17	18	20	21	$\cdots$	27	29	$\cdots$	40

$d\backslash r$	2	3	4	5	6	7	8	9	10	11	$\cdots$	36
5	4-5	6	7	8	9	10-11	11-12	12-13	13-14	15	$\cdots$	40

$d\backslash r$	2	$\cdots$	39
6	3	$\cdots$	40

We see in Table D.2 that we recover all the generalized Hamming weights for $q^s = 3$ and $m = 2$, besides the one corresponding to $d = 3$, $r = 2$. For $q^s = 3$ and $m = 3$,

Table D.4: Generalized Hamming weights for $q^s = 4$, $m = 2$.

$d\backslash r$	2	3	4	5	6	7	8	9	10	11	$\cdots$	20
1	20	21										
2	15	16	19	20	21							
3	10-11	11-12	14	15	16	18	19	20	21			
4	5-7	8	9-10	10-11	12	13	14	15	16	17	$\cdots$	
5	4	5-6	7	8	9	10	11	12	13	14	$\cdots$	
6	3	4	5	6	7	8	9	10	11	12	$\cdots$	21

Table D.5: Generalized Hamming weights for $q^s = 5$, $m = 2$.

$d\backslash r$	2	3	4	5	6	7	8	9	10	11	$\cdots$	30
1	30	31										
2	24	25	29	30	31							
3	18-19	19-20	23	24	25	28	29	30	31			
4	12-14	13-15	17-18	18-19	19-20	22	23	24	25	27	$\cdots$	
5	6-9	10	11-13	12-14	15	16-17	17-18	18-19	20	21	$\cdots$	
6	5	6-8	9	10	11-12	12-13	14	15	16	17	$\cdots$	
7	4	5	6-7	8	9	10	11	12	13	14	$\cdots$	
8	3	4	5	6	7	8	9	10	11	12	$\cdots$	31

we obtain most of the generalized Hamming weights (see Table D.3), although in some cases we cannot claim that we have the equality with the bound from Theorem D.5.7. For example, for $d = 5$, we obtain directly 30 out of the 35 generalized Hamming weights for $r > 1$ (we recall that the bound is sharp for all the values represented with dots), and for the ones for which we only have bounds, the difference between the bound from Theorem D.5.7 and the true value is at most 1.

For $q^s = 4, 5$, and $m = 2$, we show the values that we obtain in Table D.4 and Table D.5. We see that for high values of r we obtain the true values of the generalized Hamming weights, and for moderate values of d and r, even in the cases where we are not able to state what the true value is, we have a small interval of possible values due to the bounds we are using.

The tables can be further improved by using the following duality theorem for the generalized Hamming weights from [21].

Theorem D.5.16 (Duality)**.** *Let C be an $[n, k]$ code. Then*

$$\{d_r(C) : 1 \leq r \leq k\} = \{1, 2, \ldots, n\} \setminus \{n + 1 - d_r(C^\perp) : 1 \leq r \leq n - k\}.$$

The set $\{d_r(C) : 1 \leq r \leq k\}$ is called the weight hierarchy of the code C. From Theorem D.5.16, we see that the weight hierarchy of a code is completely determined by the weight hierarchy of its dual, and vice versa. As the dual of a projective Reed-Muller code is another projective Reed-Muller code (for $d \not\equiv 0 \bmod q^s - 1$), this gives us more restrictions for the possible values appearing in the previous tables.

Example D.5.17. Let $q^s = 3$, $d = 3$ and $m = 3$. Looking at Table D.3, we see that for $r = 3, 6, 11, 12$, we do not know the exact value of the corresponding generalized Hamming

weight of $\mathrm{PRM}_3(3)$. Using Theorem D.2.2, we know that $\mathrm{PRM}_3^{\perp}(3) = \mathrm{PRM}_3(3)$. We are going to use Theorem D.5.16 to obtain the true value of more of the generalized Hamming weights of $\mathrm{PRM}_3(3)$. Using Theorem D.2.1, we know that $d_1(\mathrm{PRM}_3(3)) = 9$. Therefore, by Theorem D.5.16, $n + 1 - d_1(\mathrm{PRM}_3(3)) = 41 - 9 = 32$ is not in the weight hierarchy of $\mathrm{PRM}_3(3)$. Looking at Table D.3, this implies that $d_{12}(\mathrm{PRM}_3(3)) = 31$. By the monotonicity from Theorem D.5.2, this also implies that $d_{11}(\mathrm{PRM}_3(3)) = 30$.

If we consider $d_{10}(\mathrm{PRM}_3(3)) = 27$ from Table D.3, by Theorem D.5.16 we see that $41 - 27 = 14$ is not in the weight hierarchy of $\mathrm{PRM}_3(3)$. Considering the next weight $d_{11}(\mathrm{PRM}_3(3)) = 30$, we obtain that 11 is not in the weight hierarchy. But by Theorem D.5.16, as these are consecutive generalized Hamming weights and we have the monotonicity from Theorem D.5.2, this implies that 12 and 13 are contained in the weight hierarchy of $\mathrm{PRM}_3(3)$. Thus, $d_3(\mathrm{PRM}_3(3)) = 13$. Finally, by considering $d_4(\mathrm{PRM}_3(3)) = 18$, we obtain that $41 - 18 = 23$ does not belong to the weight hierarchy of $\mathrm{PRM}_3(3)$, and therefore $d_6(\mathrm{PRM}_3(3)) = 22$. Hence, we have been able to obtain the whole weight hierarchy of $\mathrm{PRM}_3(3)$ by using the bound from Theorem D.5.7 and the general properties of the generalized Hamming weights from [21].

The ideas from Example D.5.17 can be applied to improve the previous tables. For the case $q^s = 3$, $m = 2$, the only value that we did not have exactly was $d_2(\mathrm{PRM}_3(2))$, which must be equal to 4 because $\mathrm{PRM}_3^{\perp}(2) = \mathrm{PRM}_1(2)$ and $d_1(\mathrm{PRM}_1(2)) = 9$, which means that $n + 1 - d_1(\mathrm{PRM}_1(2)) = 5$ is not in the weight hierarchy of $\mathrm{PRM}_3(2)$. For the rest of the tables, we show the improved values in Tables D.6, D.7 and D.8. We note that we obtain almost all of the exact values of the generalized Hamming weights corresponding to the previous tables for $d \not\equiv 0 \bmod q^s - 1$.

Table D.6: Improved table of the generalized Hamming weights for $q^s = 3$, $m = 3$, with $d \not\equiv 0 \bmod q^s - 1$.

$d\backslash r$	2	3	4	5	6	7	8	9	10	11	12	13	$\cdots$	20
1	36	39	40											
3	12	13	18	21	22	24	25	26	27	30	31	33	$\cdots$	40
5	4	6	7	8	9	10	11	12	13	15	16	17	$\cdots$	40

Table D.7: Improved table of the generalized Hamming weights for $q^s = 4$, $m = 2$, with $d \not\equiv 0 \bmod q^s - 1$.

$d\backslash r$	2	3	4	5	6	7	8	9	10	11	$\cdots$	18
1	20	21										
2	15	16	19	20	21							
4	5	8	9	11	12	13	14	15	16	17	$\cdots$	
5	4	5	7	8	9	10	11	12	13	14	$\cdots$	21

Table D.8: Improved table of the generalized Hamming weights for $q^s = 5$, $m = 2$, with $d \not\equiv 0 \bmod q^s - 1$.

$d\backslash r$	2	3	4	5	6	7	8	9	10	11	$\cdots$	28
1	30	31										
2	24	25	29	30	31							
3	18-19	19-20	23	24	25	28	29	30	31			
5	6	10	11	12-14	15	16	18	19	20	21	$\cdots$	
6	5	6	9	10	11	13	14	15	16	17	$\cdots$	
7	4	5	6	8	9	10	11	12	13	14	$\cdots$	31

We also note that the generalized Hamming weights of projective Reed-Muller codes seem to achieve the generalized Singleton bound D.5.3 in many cases. This can be checked in the tables by considering, for a fixed degree d, the smallest value r^* such that $d_{r+1}(\mathrm{PRM}_d(m)) - d_r(\mathrm{PRM}_d(m)) = 1$ for all $r \geq r^*$. All the generalized Hamming weights $d_r(\mathrm{PRM}_d(m))$ with $r \geq r^*$ achieve the generalized Singleton bound. For instance, in Table D.7, for $d = 4$ we have that $d_r(\mathrm{PRM}_4(2))$ achieves the generalized Singleton bound for $r \geq 5$ (in this case, $n - k + r = 21 - 15 + r = 6 + r$).

For the cases where we have $d \equiv 0 \bmod q^s - 1$, the weight hierarchy of $\mathrm{PRM}_d(m)$ gives information about the weight hierarchy of $\mathrm{PRM}_d^{\perp}(m) = \mathrm{PRM}_{d^\perp}(m) + \langle (1, \ldots, 1) \rangle$. In particular, if we consider r^* as before, then

$$d_1(\mathrm{PRM}_d^{\perp}(m)) = d_1(\mathrm{PRM}_{d^\perp}(m) + \langle (1, \ldots, 1) \rangle) = n + 2 - d_{r^*}(\mathrm{PRM}_d(m)).$$

As we are able to obtain exactly the value of the generalized Hamming weights for large values of r in all the cases that we have checked, we can obtain the minimum distance of $\mathrm{PRM}_d^{\perp}(m)$ for the case $d \equiv 0 \bmod q^s - 1$. The minimum distances of these codes are the only basic parameters missing in [20] for the family of projective Reed-Muller codes and their duals. Clearly, by using more of the generalized Hamming weights of $\mathrm{PRM}_d(m)$ we can obtain (or at least bound) more generalized Hamming weights of $\mathrm{PRM}_d^{\perp}(m)$ besides the minimum distance in the case $d \equiv 0 \bmod q^s - 1$.

Bibliography

[1] P. Beelen, M. Datta, and S. R. Ghorpade. Maximum number of common zeros of homogeneous polynomials over finite fields. *Proc. Amer. Math. Soc.*, 146(4):1451–1468, 2018.

[2] P. Beelen, M. Datta, and S. R. Ghorpade. Vanishing ideals of projective spaces over finite fields and a projective footprint bound. *Acta Math. Sin. (Engl. Ser.)*, 35(1):47–63, 2019.

[3] P. Beelen, M. Datta, and S. R. Ghorpade. A combinatorial approach to the number of solutions of systems of homogeneous polynomial equations over finite fields. *Mosc. Math. J.*, 22(4):565–593, 2022.

[4] J. Bierbrauer. The theory of cyclic codes and a generalization to additive codes. *Des. Codes Cryptogr.*, 25(2):189–206, 2002.

[5] T. Blackmore and G. H. Norton. Matrix-product codes over $\mathbb{F}_q$. *Appl. Algebra Engrg. Comm. Comput.*, 12(6):477–500, 2001.

[6] M. Boguslavsky. On the number of solutions of polynomial systems. *Finite Fields Appl.*, 3(4):287–299, 1997.

[7] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[8] M. Datta and S. R. Ghorpade. Number of solutions of systems of homogeneous polynomial equations over finite fields. *Proc. Amer. Math. Soc.*, 145(2):525–541, 2017.

[9] P. Delsarte, J.-M. Goethals, and F. J. MacWilliams. On generalized Reed-Muller codes and their relatives. *Information and Control*, 16:403–442, 1970.

[10] C. Galindo, O. Geil, F. Hernando, and D. Ruano. New binary and ternary LCD codes. *IEEE Trans. Inform. Theory*, 65(2):1008–1016, 2019.

[11] C. Galindo and F. Hernando. Quantum codes from affine variety codes and their subfield-subcodes. *Des. Codes Cryptogr.*, 76(1):89–100, 2015.

[12] C. Galindo, F. Hernando, and D. Ruano. Stabilizer quantum codes from J-affine variety codes and a new Steane-like enlargement. *Quantum Inf. Process.*, 14(9):3211–3231, 2015.

[13] P. Gimenez, D. Ruano, and R. San-José. Entanglement-assisted quantum error-correcting codes from subfield subcodes of projective Reed-Solomon codes. *Comput. Appl. Math.*, 42(8):Paper No. 363, 31, 2023.

[14] P. Gimenez, D. Ruano, and R. San-José. Subfield subcodes of projective Reed-Muller codes. *Finite Fields Appl.*, 94:Paper No. 102353, 46, 2024.

[15] M. Grassl. Bounds on the minimum distance of linear codes and quantum codes. Online available at `http://www.codetables.de`, 2007. Accessed on 2023-04-04.

[16] P. Heijnen and R. Pellikaan. Generalized Hamming weights of q-ary Reed-Muller codes. *IEEE Trans. Inform. Theory*, 44(1):181–196, 1998.

[17] T. Kasami, S. Lin, and W. W. Peterson. New generalizations of the Reed-Muller codes. I. Primitive codes. *IEEE Trans. Inform. Theory*, IT-14:189–199, 1968.

[18] G. Lachaud. Projective Reed-Muller codes. In *Coding theory and applications (Cachan, 1986)*, volume 311 of *Lecture Notes in Comput. Sci.*, pages 125–129. Springer, Berlin, 1988.

[19] C. Rentería and H. Tapia-Recillas. Reed-Muller codes: an ideal theory approach. *Comm. Algebra*, 25(2):401–413, 1997.

[20] A. B. Sørensen. Projective Reed-Muller codes. *IEEE Trans. Inform. Theory*, 37(6):1567–1576, 1991.

[21] V. K. Wei. Generalized Hamming weights for linear codes. *IEEE Trans. Inform. Theory*, 37(5):1412–1418, 1991.

Paper E

Hulls of projective Reed-Muller codes over the projective plane

Diego Ruano, Rodrigo San-José

Abstract

By solving a problem regarding polynomials in a quotient ring, we obtain the relative hull and the Hermitian hull of projective Reed-Muller codes over the projective plane. The dimension of the hull determines the minimum number of maximally entangled pairs required for the corresponding entanglement-assisted quantum error-correcting code. Hence, by computing the dimension of the hull we now have all the parameters of the symmetric and asymmetric entanglement-assisted quantum error-correcting codes constructed with projective Reed-Muller codes over the projective plane. As a byproduct, we also compute the dimension of the Hermitian hull for affine Reed-Muller codes in 2 variables.

Keywords: Projective Reed-Muller codes, hull, entanglement-assisted quantum error-correcting codes, polynomial ring.

MSC: 81P70, 94B05, 13P25.

DOI: 10.48550/arXiv.2312.13921

Reference: D. Ruano, R. San-José. Hulls of projective Reed-Muller codes over the projective plane. SIAM Journal on Applied Algebra and Geometry, to appear (2024). ArXiv 2312.13921.

Affiliation: Diego Ruano, Rodrigo San-José: IMUVA-Mathematics Research Institute, Universidad de Valladolid.

E.1 Introduction

Evaluation codes, have a rich algebraic structure and can be studied using tools from commutative algebra [16, 21, 22]. In particular, projective Reed-Muller codes are a family of evaluation codes obtained by evaluating homogeneous polynomials of a given degree at the projective space [20, 27]. In [20] it is shown that these codes can outperform affine Reed-Muller codes in some instances. Taking into account that Reed-Muller codes were one of the first families of linear codes used to construct quantum error-correcting codes (QECCs) [29], it is natural to consider projective Reed-Muller codes for constructing quantum codes. When one evaluates over the projective line, this family corresponds to projective Reed-Solomon codes, which have been used for constructing QECCs in various contexts [2, 13]. As we will see, by using evaluation codes we translate problems about quantum and classical codes to questions regarding polynomials in a quotient ring.

The importance of QECCs is growing in parallel to the interest in quantum computing, as QECCs are necessary to achieve fault tolerant computation [26]. One can construct QECCs from classical linear codes using the CSS construction and the Hermitian construction [6, 19, 28], but these constructions require to have some self-orthogonality conditions for the corresponding classical codes. Using entanglement assistance, it is possible to remove the self-orthogonality restrictions, giving rise to entanglement-assisted quantum error-correcting codes (EAQECCs) [5]. Both the CSS construction and the Hermitian construction can be generalized to this context, see Theorems E.4.1 and E.4.8 from [11] and [10], respectively.

For the CSS construction, one can consider two codes C_1 and C_2, and the minimum number required of maximally entangled quantum states is equal to $c := \dim C_1 - \dim C_1 \cap C_2^{\perp}$. Therefore, the dimension of the *relative hull of* C_1 *with respect to* C_2, defined as

$$\mathrm{Hull}_{C_2}(C_1) := C_1 \cap C_2^{\perp},$$

determines the parameter c [1]. For the Hermitian construction, we only use one code C, and the parameter c is given by $\dim C - \dim C \cap C^{\perp_h}$, where $C^{\perp_h}$ is the Hermitian dual of C. The *Hermitian hull* of C is thus defined as

$$\mathrm{Hull}^H(C) := C \cap C^{\perp_h}.$$

Going back to projective Reed-Muller codes, as they are evaluation codes, we can view their codewords as classes of polynomials in a quotient ring. This motivates Section E.3 of this paper, where we compute bases of polynomials for some appropriate subspaces of the quotient rings associated to projective Reed-Muller codes by using Gröbner bases techniques. As a consequence of this computation, we give a basis for the relative hull of projective Reed-Muller codes over the projective plane $\mathbb{P}^2$. We also estimate the dimension of the Hermitian hull, and give bases in some cases. The estimate that we obtain is sharp in all the cases we have checked. As a byproduct of these computations, we also compute the Hermitian hull of affine Reed-Muller codes in 2 variables, which was known to be trivial in some cases [12, 24], but was not known in general. With this knowledge, in Section E.4 we give the parameters of the EAQECCs obtained by using projective Reed-Muller codes over $\mathbb{P}^2$, since the dimension of the hull determines the parameter c. Although projective Reed-Muller codes had already been used to construct QECCs in some particular cases [25], the cases that required entanglement assistance had not been yet addressed. We focus on the

case of $\mathbb{P}^2$ because it offers a good trade-off between providing long codes over a small finite field and avoiding computations that are too involved, making explicit formulas unfeasible. For the general case of $\mathbb{P}^m$, one has to make additional assumptions, such as restricting to the Euclidean case and requiring $C_1 = C_2$, see [17].

E.2 Preliminaries

We consider the finite field $\mathbb{F}_q$ with q elements, and the projective space $\mathbb{P}^m$ over $\mathbb{F}_q$. Throughout this work, we will fix representatives for the points of $\mathbb{P}^m$: for each point $[Q] \in \mathbb{P}^m$, we choose the representative whose leftmost entry is equal to 1. We will denote by $P^m = \{Q_1, \ldots, Q_n\}$, with $n = |P^m| = \frac{q^{m+1}-1}{q-1}$, the set of representatives that we have chosen (seen as points in the affine space $\mathbb{A}^{m+1}$). For a set of points $A \subset \mathbb{A}^{m+1}$ we will denote by $[A]$ the set of points $\{[a_0 : \cdots : a_m] \mid (a_0, \ldots, a_m) \in A \setminus \{0\}\}$ (using the representatives that we have chosen).

We consider now the polynomial ring $S = \mathbb{F}_q[x_0, \ldots, x_m]$. The *evaluation map* is the $\mathbb{F}_q$-linear map defined by

$$\mathrm{ev} : S \to \mathbb{F}_q^n, \;\; f \mapsto (f(Q_1), \ldots, f(Q_n)) \,.$$

Let d be a positive integer. If we consider $S_d \subset S$, the set of homogeneous polynomials of degree d, we have that $\mathrm{ev}(S_d)$ is the *projective Reed-Muller code* of degree d, which we will denote by $\mathrm{PRM}_d(q, m)$, or $\mathrm{PRM}_d(m)$ if there is no confusion about the field. For a code $C \subset \mathbb{F}_q^n$, we denote its minimum distance by $\mathrm{wt}(C)$. The following results about the parameters of projective Reed-Muller codes and their duality appear in [27].

Theorem E.2.1. *The projective Reed-Muller code* $\mathrm{PRM}_d(q, m)$, $1 \leq d \leq m(q-1)$, *is an* $[n, k]$*-code with*

$$n = \frac{q^{m+1}-1}{q-1},$$
$$k = \sum_{t \equiv d \bmod q-1, 0<t\leq d} \left(\sum_{j=0}^{m+1} (-1)^j \binom{m+1}{j} \binom{t - jq + m}{t - jq} \right).$$

For the minimum distance, we have

$$\mathrm{wt}(\mathrm{PRM}_d(q, m)) = (q-s)q^{m-r-1}, \;\; \textit{where} \;\; d - 1 = r(q-1) + s, \; 0 \leq s < q - 1.$$

Theorem E.2.2. *Let* $1 \leq d \leq m(q-1)$ *and let* $d^\perp = m(q-1) - d$. *Then*

$$\mathrm{PRM}_d^\perp(q, m) = \mathrm{PRM}_{d^\perp}(q, m) \qquad \textit{if } d \not\equiv 0 \bmod q-1,$$
$$\mathrm{PRM}_d^\perp(q, m) = \mathrm{PRM}_{d^\perp}(q, m) + \langle (1, \ldots, 1) \rangle \qquad \textit{if } d \equiv 0 \bmod q-1.$$

Remark E.2.3. Theorem E.2.2 states that, if $d \not\equiv 0 \bmod q-1$ the dual of a projective Reed-Muller code is another projective Reed-Muller code. If we define $\mathrm{PRM}_0(2) = \langle (1, \ldots, 1) \rangle$, then for $d = m(q-1)$ we can also say that the dual of a projective Reed-Muller code is another projective Reed-Muller code. Hence, for $m = 2$, the case we are going to study in this paper, the only case in which the dual of a projective Reed-Muller code is not another projective Reed-Muller code is when $d = q - 1$.

With respect to affine Reed-Muller codes, we denote them by $\mathrm{RM}_d(q,m)$, or by $\mathrm{RM}_d(m)$ if there is no confusion about the field. We have the following results about their parameters and their duality from [8,18].

Theorem E.2.4. *The Reed-Muller code* $\mathrm{RM}_d(q,m)$, $0 \leq d \leq m(q-1)$, *is an* $[n,k]$*-code with*

$$n = q^m,$$
$$k = \sum_{t=0}^{d} \sum_{j=0}^{m} (-1)^j \binom{m}{j} \binom{t-jq+m-1}{t-jq}.$$

For the minimum distance, we have

$$\mathrm{wt}(\mathrm{RM}_d(q,m)) = (q-s)q^{m-r-1}, \text{ where } d = r(q-1)+s,\ 0 \leq s < q-1.$$

Theorem E.2.5. *Let* $0 \leq d \leq m(q-1)$. *Then*

$$\mathrm{RM}_d^{\perp}(q,m) = \mathrm{RM}_{m(q-1)-d-1}(q,m).$$

Going back to projective Reed-Muller codes, we have seen that $\mathrm{PRM}_d(m) = \mathrm{ev}(S_d)$, which gives the isomorphism

$$\mathrm{PRM}_d(m) \cong S_d/(I(P^m) \cap S_d) \cong (S_d + I(P^m))/I(P^m),$$

where $I(P^m)$ is the vanishing ideal of P^m. This is because, if we restrict ev to S_d, the polynomials in the kernel are precisely the polynomials from S_d that vanish at each of the points of P^m, which are the polynomials in $I(P^m) \cap S_d$. This isomorphism allows us to view the vectors of the code as polynomials in a quotient ring. It is important to note that two polynomials in $S/I(P^m)$ have the same evaluation if and only if their classes in $S/I(P^m)$ are the same. This is why we can discuss linear independence both in $\mathrm{PRM}_d(m) \subset \mathbb{F}_q^n$ and in $S/I(P^m)$.

Moreover, we can express many important aspects of the code purely in terms of polynomials, for example the minimum distance [16] or their duals [21]. The theory of Gröbner bases is one of the main tools that are used for studying evaluation codes using this approach. In the rest of this section, we introduce some of the Gröbner-related results for projective Reed-Muller codes that we will use in the rest of the paper.

In what follows, we will abuse the notation and denote $S_d/I(P^m) = (S_d+I(P^m))/I(P^m)$. Moreover, for a polynomial $f \in S$, we will use the same notation f for both the polynomial and its class in $S/I(P^m)$. We refer the reader to [7] for the basic concepts of Gröbner bases. For $f \in S$, we denote by $\mathrm{in}(f)$ the leading monomial of f (without the coefficient). For an ideal $I \subset S$, $\mathrm{in}(I)$ denotes the ideal generated by the leading monomials of the polynomials in I. We have the following result for the vanishing ideal of P^m from [14].

Theorem E.2.6. *The vanishing ideal of* P^m *is generated by the following polynomials:*

$$\begin{aligned} I(P^m) = &\langle x_0^2 - x_0, x_1^q - x_1, x_2^q - x_2, \ldots, x_m^q - x_m, (x_0-1)(x_1^2-x_1), \\ &(x_0-1)(x_1-1)(x_2^2-x_2), \ldots, (x_0-1)\cdots(x_{m-1}^2 - x_{m-1}), (x_0-1)\cdots(x_m-1)\rangle. \end{aligned}$$

Moreover, these generators form a universal Gröbner basis of the ideal $I(P^m)$ *(i.e., they form a Gröbner basis for any monomial order), and we have that*

$$\mathrm{in}(I(P^m)) = \langle x_0^2, x_1^q, x_2^q, \ldots, x_m^q, x_0x_1^2, x_0x_1x_2^2, \ldots, x_0x_1\cdots x_{m-1}^2, x_0x_1\cdots x_m\rangle.$$

In this work we will study the case $m = 2$, in which we have

$$I(P^2) = \langle x_0^2 - x_0, x_1^q - x_1, x_2^q - x_2, (x_0 - 1)(x_1^2 - x_1), (x_0 - 1)(x_1 - 1)(x_2 - 1)\rangle.$$

We introduce now the bases of polynomials that we will use in the following sections.

Lemma E.2.7. *Let $1 \leq d \leq 2(q-1)$. We consider the following sets of monomials:*

$$\begin{aligned} A_1^d &= \{x_0^{a_0} x_1^{a_1} x_2^{a_2} \mid a_0 > 0, a_0 + a_1 + a_2 = d, 0 \leq a_1, a_2 \leq q-1\}, \\ A_2^d &= \{x_1^{a_1} x_2^{a_2} \mid a_1 > 0, a_1 + a_2 = d, 0 \leq a_2 \leq q-1\}, \\ A_3^d &= \{x_2^d\}. \end{aligned}$$

Then, $A^d = A_1^d \cup A_2^d \cup A_3^d$ forms a basis for $S_d/I(P^2)$.

Proof. A^d is a basis for $S_d/I(\mathbb{P}^2)_d$ (for example, see [3]), where $I(\mathbb{P}^2)$ is the vanishing ideal of $\mathbb{P}^2$, i.e, the ideal generated by the homogeneous polynomials that vanish in all the points of $\mathbb{P}^2$. Therefore, the image by the evaluation map of A^d is a basis for $\mathrm{PRM}_d(2)$, which means that the classes of these polynomials in $S/I(P^2)$ are also a basis for $S_d/I(P^2)$. □

Remark E.2.8. Let $1 \leq d \leq 2(q-1)$ and $k = \dim \mathrm{RM}_{d-1}(2)$. Then it is clear that $\left|A_1^d\right| = k$, and the previous result shows that we have the following formula:

$$\dim \mathrm{PRM}_d(2) = \begin{cases} k + d + 1 & \text{if } 1 \leq d \leq q-1, \\ k + q + 1 & \text{if } q \leq d < 2(q-1). \end{cases}$$

From [14], we have the following lemma about $S/I(P^2)$.

Lemma E.2.9. *The set of monomials $\{x_1^{a_1} x_2^{a_2}, x_0 x_2^{a_2}, x_0 x_1 \mid 0 \leq a_i \leq q-1, 1 \leq i \leq 2\}$ is a basis for $S/I(P^2)$.*

We show now how to express any monomial from A^d in terms of the basis from Lemma E.2.9. The following definition is useful for this purpose.

Definition E.2.10. For an integer $z \geq 0$, we denote by $\overline{z}$ the integer $1 \leq \overline{z} \leq q-1$ such that $\overline{z} \equiv z \bmod q-1$ if $z > 0$, and $\overline{z} = 0$ if $z = 0$.

Remark E.2.11. Any monomial $x_0^{\alpha_0} x_1^{\alpha_1} x_2^{\alpha_2}$ with $\alpha_0 > 0$ is equivalent to $x_0^{\alpha_0'} x_1^{\alpha_1} x_2^{\alpha_2}$ in $S/I(P^2)$, for any $\alpha_0' > 0$, because we have the polynomial $x_0^2 - x_0$ in $I(P^2)$. In particular, $x_0^{\alpha_0} x_1^{\alpha_1} x_2^{\alpha_2}$ is equivalent to $x_0 x_1^{\alpha_1} x_2^{\alpha_2}$ if $\alpha_0 > 0$. Moreover, in Definition E.2.10 we treat the case $z = 0$ separately so that we have

$$x_0^{a_0} x_1^{a_1} x_2^{a_2} \equiv x_0^{\overline{a_0}} x_1^{\overline{a_1}} x_2^{\overline{a_2}} \bmod I(P^2),$$

for any $0 \leq a_0, a_1, a_2 \leq 2(q-1)$. Notice that, for evaluation codes, having exponent $q-1$ is not the same as 0 since, for instance,

$$x_0^0 = 1 \not\equiv x_0^{q-1} \bmod I(P^2).$$

This can be checked by evaluating 1 and x_0^{q-1} at any point of the form $(0, 1, x_2)$, $x_2 \in \mathbb{F}_q$ (recall that two polynomials are equivalent modulo $I(P^2)$ if and only if they have the same evaluation).

The following Lemma from [14] shows how to express any monomial in terms of the basis from Lemma E.2.9.

Lemma E.2.12. *Let a_0, a_1, a_2 be integers.*

1. *If $a_0 = 0$, then*
$$x_1^{a_1} x_2^{a_2} \equiv x_1^{\overline{a_1}} x_2^{\overline{a_2}} \bmod I(P^2).$$
2. *If $a_1 = 0$, then*
$$x_0^{a_0} x_2^{a_2} \equiv x_0 x_2^{\overline{a_2}} \bmod I(P^2).$$
3. *If $a_0 > 0$ and $a_1 > 0$, then*
$$\begin{aligned} x_0^{a_0} x_1^{a_1} x_2^{a_2} &\equiv x_1^{\overline{a_1}} x_2^{\overline{a_2}} + x_0 x_2^{\overline{a_2}} - x_2^{\overline{a_2}} + x_0 x_1 - x_0 - x_1 + 1 \bmod I(P^2) \\ &\equiv x_1^{\overline{a_1}} x_2^{\overline{a_2}} + (x_0 - 1)(x_2^{\overline{a_2}} + x_1 - 1) \bmod I(P^2). \end{aligned}$$

In particular, Lemma E.2.12 allows us to express all the monomials from the basis in Lemma E.2.7 in terms of the basis from Lemma E.2.9. This is crucial because the idea of the next section is, for $1 \leq d_1 \leq d_2 \leq 2(q-1)$, to consider the bases from Lemma E.2.7 for $S_{d_1}/I(P^2)$ and $S_{d_2}/I(P^2)$, and express them in terms of the basis for $S/I(P^2)$ from Lemma E.2.9 using Lemma E.2.12. Once we have all the polynomials expressed in this way, it is easier to find the polynomials lying in $S_{d_1}/I(P^2) \cap S_{d_2}/I(P^2)$, which, as we will see, determines the relative hull of $\mathrm{PRM}_{d_1}(2)$ and $\mathrm{PRM}_{d_2}(2)$. For the Hermitian case, the ideas are also very similar, although the computations are more involved.

E.3 Computing the hulls of projective Reed-Muller codes

The aim of this section is to obtain bases for the relative hull and Hermitian hull of projective Reed-Muller codes. We do this by computing first a basis of polynomials for some appropriate subspaces of $S/I(P^2)$. We deduce, in particular, the dimension of the hull, which will determine the entanglement parameter c for the EAQECCs constructed with projective Reed-Muller codes in Section E.4.

E.3.1 Euclidean hull

In this subsection we compute a basis for $\mathrm{Hull}_{C_2}(C_1) = C_1 \cap C_2^{\perp}$, the relative hull of C_1 and C_2, when $C_i = \mathrm{PRM}_{d_i}(2)$, for $i = 1, 2$. For $\mathrm{PRM}_{d_2}^{\perp}(2)$, by Theorem E.2.2 we have that, if $d_2 \neq q-1$, then $\mathrm{PRM}_{d_2}^{\perp}(2) = \mathrm{PRM}_{d_2^{\perp}}(2)$, where $d_2^{\perp} = 2(q-1) - d_2$ (assuming $\mathrm{PRM}_0(2) = \langle (1, \ldots, 1) \rangle$). We avoid the case where $d_2 = q-1$ because, by Theorem E.2.2, in that case we have $\mathrm{PRM}_{d_2}^{\perp}(2) = \mathrm{PRM}_{d_2^{\perp}}(2) + \langle (1, \ldots, 1) \rangle$, which is no longer isomorphic to $S_{d_2^{\perp}}/I(P^2)$. Assuming $d_2 \neq q-1$, the problem of obtaining a basis for $\mathrm{PRM}_{d_1}(2) \cap \mathrm{PRM}_{d_2}^{\perp}(2)$ becomes equivalent to computing a basis for $\mathrm{PRM}_{d_1}(2) \cap \mathrm{PRM}_{d_2}(2)$, for any $1 \leq d_1 \leq d_2 \leq 2(q-1)$, $d_2 \neq q-1$, and that is the problem we solve in what follows. In [25, Thm. 10.7] the authors construct quantum codes using pairs of projective Reed-Muller codes such that the dual of one of the codes is contained in the other. In particular, they obtain the following result.

Lemma E.3.1. *Let $1 \leq d_1 \leq d_2 \leq m(q-1)$. If $d_1 \equiv d_2 \bmod q-1$, then $\mathrm{PRM}_{d_1}(m) \subset \mathrm{PRM}_{d_2}(m)$.*

Therefore, when $d_1 \equiv d_2 \bmod q-1$, with $d_2 \neq q-1$, the relative hull is straightforward to obtain. To avoid making exceptions in many of the following results, we exclude the case $d_1 \equiv d_2 \bmod q-1$, which is already covered by Lemma E.3.1.

Because of the isomorphism $S_{d_i}/I(P^2) \cong \mathrm{PRM}_{d_i}(2)$, for $i = 1, 2$, the problem of computing a basis for $\mathrm{PRM}_{d_1}(2) \cap \mathrm{PRM}_{d_2}(2)$ can be understood as computing a basis for $S_{d_1}/I(P^2) \cap S_{d_2}/I(P^2)$, as a subspace of $S/I(P^2)$. Hence, computing the dimension of $S_{d_1}/I(P^2) \cap S_{d_2}/I(P^2)$ for arbitrary $1 \leq d_1 \leq d_2 \leq 2(q-1)$ gives the parameter c for any pair of projective Reed-Muller codes over P^2 (except when we have $d_2 = q-1$). We give now some preliminary results.

Lemma E.3.2. *We have that $1 \notin S_d/I(P^2)$ for $1 \leq d \leq 2(q-1)$.*

Proof. If $d \leq q-1$ and we had $1 \in S_d/I(P^2)$, then we would have the evaluation of $x_0^d - 1$ in $\mathrm{PRM}_d(2)$, which has Hamming weight $q^2+q+1-q^2 = q+1 < (q-d+1)q = \mathrm{wt}(\mathrm{PRM}_d(2))$. For $q \leq d \leq 2(q-1)$, if we had $1 \in S_d/I(P^2)$, then we would also have the evaluation of $x_0^d - x_0^{q-1}x_1^{d-(q-1)} + x_1^d - 1 \equiv x_0^d + (1-x_0)x_1^d - 1 \bmod I(P^2)$ in $\mathrm{PRM}_d(2)$ (recall Remark E.2.11), which has Hamming weight $1 < \mathrm{wt}(\mathrm{PRM}_d(2))$. □

Let $f \in S_{d_1}$. The following lemmas show when we have $f \in S_{d_2}/I(P^2)$ depending on the monomials that are in the support of f. This will allow us to determine which polynomials are in $S_{d_1}/I(P^2) \cap S_{d_2}/I(P^2)$ and, thus, to obtain a basis.

Lemma E.3.3. *Let $1 \leq d_1 < d_2 \leq 2(q-1)$. We have that the classes of the monomials in $A_1^{d_1}$ are contained in $S_{d_2}/I(P^2)$.*

Proof. Let $x_0^{a_0}x_1^{a_1}x_2^{a_2} \in A_1^{d_1}$. Then $x_0^{a_0+d_2-d_1}x_1^{a_1}x_2^{a_2} \in S_{d_2}/I(P^2)$, and $x_0^{a_0}x_1^{a_1}x_2^{a_2} \equiv x_0^{a_0+d_2-d_1}x_1^{a_1}x_2^{a_2} \bmod I(P^2)$ by Remark E.2.11. □

Let $1 \leq d_1 < d_2 \leq 2(q-1)$. We note that the monomials in $A_1^{d_1}$ and $A_1^{d_2}$ generate $\mathrm{RM}_{d_1-1}(2)$ and $\mathrm{RM}_{d_2-1}(2)$, respectively, when considering their evaluation in $[\{1\} \times \mathbb{F}_q^2]$. Thus, $\dim\left(S_{d_1}/I(P^2) \cap S_{d_2}/I(P^2)\right) \geq \dim \mathrm{RM}_{d_1-1}(2)$.

Example E.3.4. Let $\mathbb{F}_q = \mathbb{F}_4$, and we consider $d_1 = 4 < 5 = d_2$. By Lemma E.3.3, we have that A_1^4 is in $S_4/I(P^2) \cap S_5/I(P^2)$. In this case, we have

$$A_1^4 = \{x_0^4, x_0^3x_1, x_0^3x_2, x_0^2x_1^2, x_0^2x_1x_2, x_0^2x_2^2, x_0x_1^3, x_0x_1^2x_2, x_0x_1x_2^2, x_0x_2^3\}.$$

If we multiply all the elements of A_1^4 by x_0, we obtain a set of monomials of degree 5 which have the same evaluation at P^2 as these monomials (see Remark E.2.11).

Lemma E.3.5. *Let $1 \leq d_1 < d_2 \leq 2(q-1)$ with $d_1 \not\equiv d_2 \bmod q-1$. Let $f \in S_{d_1}$ such that it only has monomials from $A_2^{d_1}$ in its support, i.e., it can be expressed as*

$$f = \sum_{a_1+a_2=d_1, 0<a_1, 0\leq a_2\leq q-1} \lambda_{a_1,a_2}x_1^{a_1}x_2^{a_2}, \lambda_{a_1,a_2} \in \mathbb{F}_q.$$

Let $Y = \{0, 1, \ldots, \min\{d_1-1, d_2-q\}\}$ and $Y_f = \{0 \leq a_2 \leq q-1 \mid \lambda_{d_1-a_2,a_2} \neq 0\}$. Then $f \in S_{d_2}/I(P^2)$ if and only if $Y_f \subset Y$.

Proof. Assuming that $f \in S_{d_2}/I(P^2)$, there is also an expression

$$f \equiv \sum_{x_0^{a_0}x_1^{a_1}x_2^{a_2} \in A^{d_2}} \gamma_{a_0,a_1,a_2} x_0^{a_0}x_1^{a_1}x_2^{a_2} \bmod I(P^2), \gamma_{a_0,a_1,a_2} \in \mathbb{F}_q. \tag{E.3.1}$$

We have $f(0,0,1) = 0$, which means that $\gamma_{0,0,d_2} = 0$. We consider now a monomial order with $x_0 < x_1 < x_2$, and let $\mathrm{in}(f) = x_1^{a_1}x_2^{a_2} \equiv x_1^{\overline{a_1}}x_2^{a_2} \bmod I(P^2)$, with $a_1 > 0$, $0 \leq a_2 \leq q-1$ and $a_1 + a_2 = d_1$. Therefore, because of (E.3.1), we must have some monomial in A^{d_2} such that its expression in the basis from Lemma E.2.9 contains $x_1^{\overline{a_1}}x_2^{a_2}$ in its support. The only monomials that satisfy that are $x_1^{\overline{a_1}+q-1}x_2^{a_2}$ if $d_2 = \overline{a_1}+a_2+(q-1)$, or $x_0^{c_0}x_1^{\overline{a_1}}x_2^{a_2}$, with $c_0 = d_2 - \overline{a_1} - a_2 > 0$. In the first case, we have $d_1 \equiv d_2 \bmod q-1$, but we are assuming $d_1 \not\equiv d_2 \bmod q-1$. In the other case, by Lemma E.2.12 we have

$$x_0^{c_0}x_1^{\overline{a_1}}x_2^{a_2} \equiv x_1^{\overline{a_1}}x_2^{a_2} + (x_0-1)(x_2^{a_2} + x_1 - 1) \bmod I(P^2).$$

Hence, to obtain $x_1^{\overline{a_1}}x_2^{a_2}$ in the right-hand side of (E.3.1), we must have $\gamma_{c_0,\overline{a_1},a_2} = \lambda_{a_1,a_2}$. We denote now $(A^{d_2})^{(1)} := A^{d_2} \setminus \{x_0^{c_0}x_1^{\overline{a_1}}x_2^{a_2}\}$. We obtain

$$\begin{aligned} f^{(1)} =& f - \lambda_{a_1,a_2}x_1^{a_1}x_2^{a_2} \\ \equiv& \sum_{x_0^{\alpha_0}x_1^{\alpha_1}x_2^{\alpha_2} \in (A^{d_2})^{(1)}} \gamma_{\alpha_0,\alpha_1,\alpha_2}x_0^{\alpha_0}x_1^{\alpha_1}x_2^{\alpha_2} + \gamma_{c_0,\overline{a_1},a_2}(x_0-1)(x_2^{a_2}+x_1-1) \bmod I(P^2). \end{aligned} \tag{E.3.2}$$

Now we have $\mathrm{in}(f^{(1)}) < \mathrm{in}(f)$. We can consider $\mathrm{in}(f^{(1)}) = x_1^{b_1}x_2^{b_2}$ and argue as before to obtain a polynomial $f^{(2)}$ such that $\mathrm{in}(f^{(2)}) < \mathrm{in}(f^{(1)})$, which can be expressed as in (E.3.2) in terms of a set $(A^{d_2})^{(2)} = A^{d_2} \setminus \{x_0^{c_0}x_1^{\overline{a_1}}x_2^{a_2}, x_0^{c_0'}x_1^{\overline{b_1}}x_2^{b_2}\}$.

We can do this until we get $f^{(l)} = 0$ for some $l \geq 0$. At that step, we have

$$0 \equiv \sum_{x_0^{\alpha_0}x_1^{\alpha_1}x_2^{\alpha_2} \in (A^{d_2})^{(l)}} \gamma_{\alpha_0,\alpha_1,\alpha_2}x_0^{\alpha_0}x_1^{\alpha_1}x_2^{\alpha_2} + (x_0-1)\sum_{a_2 \in Y_f} \gamma_{c_0,\overline{a_1},a_2}(x_2^{a_2}+x_1-1) \bmod I(P^2), \tag{E.3.3}$$

where $Y_f = \{0 \leq a_2 \leq q-1 \mid \lambda_{d_1-a_2,a_2} \neq 0\}$. With this notation, we have that $(A^{d_2})^{(l)} = A^{d_2} \setminus \bigcup_{a_2 \in Y_f}\{x_0^{d_2-(\overline{d_1-a_2})-a_2}x_1^{\overline{d_1-a_2}}x_2^{a_2}\}$. If we express all the monomials in (E.3.3) in terms of the basis from Lemma E.2.9, then we must have the coefficient of each element of the basis equal to 0. The monomials from (E.3.3) in the second sum are already expressed in terms of the basis from Lemma E.2.9. If we focus on the monomial $x_2^{a_2}$ for some $a_2 \in Y_f$ with $a_2 > 0$, we see that all the monomials $x_0^{\alpha_0}x_1^{\alpha_1}x_2^{a_2} \in (A^{d_2})^{(l)}$ with $0 < \alpha_0$, $0 < \alpha_1 \leq q-1$, $\alpha_1 \neq \overline{d_1 - a_2}$, and $\alpha_0 + \alpha_1 + a_2 = d_2$, have $x_2^{a_2}$ in their expression in terms of the basis from Lemma E.2.9 by Lemma E.2.12:

$$x_0^{\alpha_0}x_1^{\alpha_1}x_2^{a_2} \equiv x_1^{\alpha_1}x_2^{a_2} + (x_0-1)(x_2^{a_2}+x_1-1) \bmod I(P^2). \tag{E.3.4}$$

In fact, these are the only monomials from $(A^{d_2})^{(l)}$ with $x_2^{a_2}$ in their expression (note that the monomial with $\alpha_1 = \overline{d_1 - a_2}$ is not in $(A^{d_2})^{(l)}$). However, if we have $\gamma_{\alpha_0,\alpha_1,a_2} \neq 0$, some other monomial from $(A^{d_2})^{(l)}$ must cancel the monomial $x_1^{\alpha_1}x_2^{a_2}$ that appears in (E.3.4) from (E.3.3). The only other monomial in $(A^{d_2})^{(l)}$ with $x_1^{\alpha_1}x_2^{a_2}$ in its support when expressed in terms of the basis from Lemma E.2.9 is $x_1^{\alpha_1+q-1}x_2^{a_2}$, if $\alpha_1 + a_2 + q - 1 = d_2$ (which implies $\alpha_0 = q-1$).

Therefore, if $d_2 \leq q-1$, given $a_2 \in Y_f$, $a_2 > 0$, the monomial $x_2^{a_2}$ from (E.3.3) cannot be cancelled with any monomial from $(A^{d_2})^{(l)}$, which means that we must have $\gamma_{c_0,\overline{a_1},a_2} = \lambda_{a_1,a_2} = 0$, a contradiction with the fact that $a_2 \in Y_f$. This means that there is no $a_2 \in Y_f$ with $a_2 > 0$. Taking this into account, the only possible term in the second sum of (E.3.3) corresponds to the case $a_2 = 0$, and we have $\gamma_{c_0,\overline{a_1},a_2}(x_0-1)(x^{a_2}+x_1-1) = \gamma_{c_0,\overline{d_1},0}(x_0-1)x_1$. This polynomial cannot be generated by polynomials from A^{d_2} because its evaluation has Hamming weight $q^2+q+1-q^2-1 = q < \mathrm{wt}(\mathrm{PRM}_{d_2}(2))$ if $d_2 \leq q-1$. Thus, if $d_2 \leq q-1$, we have must have $Y_f = \emptyset$ and $f = 0$.

Lets assume now that $d_2 \geq q$. For each $a_2 \in Y_f$ with $a_2 < \overline{d_2}$, we can consider $\alpha_1 = \overline{d_2} - a_2 > 0$. We have seen that

$$x_0^{\alpha_0} x_1^{\alpha_1} x_2^{a_2} - x_1^{\alpha_1+q-1} x_2^{a_2} \equiv (x_0-1)(x_2^{a_2} + x_1 - 1) \bmod I(P^2).$$

Note that in the monomials that we have excluded to obtain $(A^{d_2})^{(l)}$ from A^{d_2}, we have that the exponent of x_1 is equivalent to $d_1 - a_2$ modulo $q-1$. The α_1 that we have chosen in this case is equivalent to $d_2 - a_2$ modulo $q-1$, which means that the corresponding monomial is still in $(A^{d_2})^{(l)}$, unless $d_1 \equiv d_2 \bmod q-1$, which is the case that we do not cover. Hence, for every $a_2 \in Y_f$ with $a_2 < \overline{d_2}$, if we choose $\gamma_{\alpha_0,\alpha_1,a_2} = -\gamma_{0,\alpha_1+q-1,a_2} = \lambda_{d_1-a_2,a_2}$, the polynomial $(x_0-1)(x_2^{a_2} + x_1 - 1)$ is cancelled from (E.3.3). If we had some $a_2 \in Y_f$ with $a_2 \geq \overline{d_2}$, we can argue as in the previous case and obtain that $\lambda_{d_1-a_2,a_2} = 0$, a contradiction.

We also have that $a_2 \leq d_1 - 1$ for every $a_2 \in Y_f$. Therefore, $Y_f \subset \{0, 1, \ldots, \min\{d_1 - 1, \overline{d_2} - 1\}\}$. Thus, $Y_f \subset Y = \{0, 1, \ldots, \min\{d_1 - 1, d_2 - q\}\}$, where if $d_2 - q < 0$ we understand that $Y = \emptyset$, which covers the case with $d_2 \geq q$ and the case with $d_2 \leq q - 1$.

On the other hand, let $f \in S_{d_1}$ such that it only has monomials from $A_2^{d_1}$ in its support, and with $Y_f \subset Y$. For each $a_2 \in Y_f$ we have

$$x_1^{d_1-a_2} x_2^{a_2} \equiv x_1^{d_2-a_2} x_2^{a_2} - x_0^{d_2-\overline{d_2}} x_1^{\overline{d_2}-a_2} x_2^{a_2} + x_0^{d_2-d_1} x_1^{d_1-a_2} x_2^{a_2} \bmod I(P^2).$$

This is easy to check because both sides have the same evaluation at $P^2 = [\{1\} \times \mathbb{F}_q^2] \cup [\{0\} \times \{1\} \times \mathbb{F}_q] \cup \{[0:0:1]\}$. Hence, $x_1^{d_1-a_2} x_2^{a_2} \in S_{d_1}/I(P^2) \cap S_{d_2}/I(P^2)$ for each $a_2 \in Y_f$, which means that $f \in S_{d_1}/I(P^2) \cap S_{d_2}/I(P^2)$. □

Example E.3.6. We continue with Example E.3.4. Using the notation from Lemma E.3.5, we have $Y = \{0, 1\}$ and we obtain that the set of monomials $\{x_1^4, x_1^3 x_2\}$ is contained in $S_4/I(P^2) \cap S_5/I(P^2)$. In fact, following the proof of Lemma E.3.5, we have that

$$x_1^4 \equiv x_1^5 - x_0^3 x_1^2 + x_0 x_1^4 \bmod I(P^2),$$

$$x_1^3 x_2 \equiv x_1^4 x_2 - x_0^3 x_1 x_2 + x_0 x_1^3 x_2 \bmod I(P^2).$$

These equivalences can be easily checked by evaluating both sides at $P^2 = [\{1\} \times \mathbb{F}_4^2] \cup [\{0\} \times \{1\} \times \mathbb{F}_4] \cup \{[0:0:1]\}$.

Lemma E.3.7. *Let $1 \leq d_1 < d_2 \leq 2(q-1)$ such that $d_1 \not\equiv d_2 \bmod q-1$. There is some $f \in S_{d_1}$ with $x_2^{d_1}$ in its support and such that $f \in S_{d_2}/I(P^2)$ if and only if $d_1 \geq q$.*

Proof. Let $f \in S_{d_1}$. By Lemma E.3.3, if there is some monomial from $A_1^{d_1}$ in the support of f, we can consider the polynomial f' obtained by subtracting that monomial from f,

and $f' \in S_{d_2}/I(P^2)$ if and only if $f \in S_{d_2}/I(P^2)$. Therefore, we can assume that the support of f is contained in $A_2^{d_1} \cup A_3^{d_1}$, i.e., it can be expressed as

$$f = \sum_{a_1+a_2=d_1, 0<a_1, 0\leq a_2\leq q-1} \lambda_{a_1,a_2} x_1^{a_1} x_2^{a_2} + \lambda_{0,d_1} x_2^{d_1}, \lambda_{a_1,a_2} \in \mathbb{F}_q.$$

We assume that $\lambda_{0,d_1} \neq 0$. As in the previous result, we must have an expression

$$f \equiv \sum_{x_0^{a_0}x_1^{a_1}x_2^{a_2} \in A^{d_2}} \gamma_{a_0,a_1,a_2} x_0^{a_0} x_1^{a_1} x_2^{a_2} \bmod I(P^2), \gamma_{a_0,a_1,a_2} \in \mathbb{F}_q. \tag{E.3.5}$$

The only monomials in A^{d_2} with $x_2^{\overline{d_1}}$ in their expression in terms of the basis from Lemma E.2.9 are $x_0^{a_0} x_1^{a_1} x_2^{\overline{d_1}}$, for some $0 < a_0$, $0 < a_1 \leq q-1$, such that $a_0 + a_1 + \overline{d_1} = d_2$, and $x_2^{d_2}$ if $d_1 \equiv d_2 \bmod q-1$, which is the case that we do not cover. Therefore, we focus on the first type of monomials, which by Lemma E.2.12 can be expressed as

$$x_0^{a_0} x_1^{a_1} x_2^{\overline{d_1}} \equiv x_1^{a_1} x_2^{\overline{d_1}} + (x_0 - 1)(x_2^{\overline{d_1}} + x_1 - 1) \bmod I(P^2). \tag{E.3.6}$$

If $d_1 \leq q-1$, we have $\overline{d_1} = d_1$ and the monomials $x_1^{a_1} x_2^{d_1}$ have degree greater than d_1. Thus, they cannot be in the support of f and they have to be cancelled in the expression from (E.3.5) if we consider some monomial $x_0^{a_0} x_1^{a_1} x_2^{d_1}$. The only other monomial in A^{d_2} with $x_1^{a_1} x_2^{d_1}$ in its expression from the basis from Lemma E.2.9 is $x_1^{a_1+q-1} x_2^{d_1}$ if $d_2 = a_1 + d_1 + q - 1$. We have $a_1 > 0$, which implies $d_2 - d_1 - (q-1) = a_1 > 0$. We also have that $a_0 + a_1 + d_1 = d_2$, which means that $a_0 = q-1$, and the only monomial that we can consider then is $x_0^{q-1} x_1^{d_2-d_1-(q-1)} x_2^{d_1}$ if $d_2 - d_1 - (q-1) > 0$. From (E.3.6) we obtain

$$x_2^{d_1} \equiv x_1^{d_2-d_1} x_2^{d_1} - x_0^{q-1} x_1^{d_2-d_1-(q-1)} x_2^{d_1} + (x_0-1)(x_1-1) + x_0 x_2^{d_1} \bmod I(P^2).$$

We have seen that $x_0^{q-1} x_1^{d_2-d_1-(q-1)} x_2^{d_1}$ is the only monomial that we can consider to obtain the monomial $x_2^{d_1}$ in the right hand side of (E.3.5), and we need to consider $x_1^{d_2-d_1} x_2^{d_1}$ with the opposite coefficient to cancel the monomial $x_1^{d_2-d_1-(q-1)} x_2^{d_1}$ (the expression of $x_1^{d_2-d_1} x_2^{d_1}$ in terms of the basis from Lemma E.2.9), i.e., we must have $-\gamma_{q-1,d_2-d_1-(q-1),d_1} = \gamma_{0,d_2-d_1,d_1} = \lambda_{0,d_1}$. We can define in this case $(A^{d_2})^{(1)} = A^{d_2} \backslash \{x_0^{q-1} x_1^{d_2-d_1-(q-1)} x_2^{d_1}, x_1^{d_2-d_1} x_2^{d_1}\}$, and consider

$$\begin{aligned} f^{(1)} =& f - \lambda_{0,d_1} x_2^{d_1} \\ \equiv& \sum_{x_0^{\alpha_0}x_1^{\alpha_1}x_2^{\alpha_2} \in (A^{d_2})^{(1)}} \gamma_{\alpha_0,\alpha_1,\alpha_2} x_0^{\alpha_0} x_1^{\alpha_1} x_2^{\alpha_2} - \lambda_{0,d_1} \left((x_0-1)(x_1-1) + x_0 x_2^{d_1}\right) \bmod I(P^2). \end{aligned} \tag{E.3.7}$$

Now $f^{(1)}$ only has monomials from $A_2^{d_1}$ in its support, and we can argue as we did in Lemma E.3.5 to obtain $f^{(l)} = 0$ after $l \geq 0$ steps. Taking into account that $d_1 \leq q-1$, we see that the monomials left in the support of $f^{(1)}$ are of the type $x_1^{a_1} x_2^{a_2}$ with $a_1 + a_2 = d_1$, $0 < a_1$, which implies that $a_2 \leq d_1 - 1$. Therefore, in the process of obtaining $f^{(l)}$ we do not need to use the monomials that we have used to obtain $f^{(1)}$ because those monomials have d_1 as the exponent for x_2. Hence, after l steps we obtain an expression similar to (E.3.3), but with the extra term $-\lambda_{0,d_1}\left((x_0-1)(x_1-1) + x_0 x_2^{d_1}\right)$ in the right

hand side. The same argument proves that we can only have $\lambda_{d_1-a_2,a_2} \neq 0$ if $a_2 \in Y = \{0, 1, \ldots, \min\{d_1-1, d_2-q\}\}$. If we are in that situation, then we can cancel all the terms in the second sum of the right hand side in (E.3.3). Thus, in that case, we would obtain a sum of monomials in $(A^{d_2})^{(l)}$ equal to $\lambda_{0,d_1}\left((x_0-1)(x_1-1)+x_0x_2^{d_1}\right)$. This implies that we have the evaluation of $(x_0-1)(x_1-1)+x_0x_2^{d_1}$ in $\mathrm{PRM}_{d_2}(2)$. This is a contradiction because we have the evaluation of $x_0^{d_2-d_1}x_2^{d_1}$ in $\mathrm{PRM}_{d_2}(2)$, and $(x_0-1)(x_1-1)+x_0x_2^{d_1}-x_0^{d_2-d_1}x_2^{d_1} \equiv (x_0-1)(x_1-1) \bmod I(P^2)$, whose evaluation has Hamming weight 1. This means that we cannot have $d_1 \leq q-1$ and $x_2^{d_1}$ in the support of f simultaneously.

On the other hand, if $d_1 \geq q$, we consider the following polynomials:

$$\begin{aligned} Q_{d_1,d_2} &:= x_2^{d_1} + x_1^{d_1-\overline{d_2}}x_2^{\overline{d_2}} + x_0^{d_1-\overline{d_2}}x_2^{\overline{d_2}} + x_0^{d_1-\overline{d_2}}x_1^{\overline{d_2}-\overline{d_1}}x_2^{\overline{d_1}} \in S_{d_1}, \\ Q'_{d_2,d_1} &:= x_2^{d_2} + x_1^{d_2-\overline{d_1}}x_2^{\overline{d_1}} + x_0^{d_2-\overline{d_1}}x_2^{\overline{d_1}} + x_0^{d_2-d_1}x_1^{d_1-\overline{d_2}}x_2^{\overline{d_2}} \in S_{d_2}. \end{aligned} \tag{E.3.8}$$

These polynomials are obtained by realising that if $x_2^{d_1}$ is in the support of f, then we must also have $x_2^{d_2}$ in (E.3.5) to obtain $f(0,0,1) \neq 0$, and adding monomials to obtain polynomials with the same evaluation at P^2, we arrive at the polynomials Q_{d_1,d_2} and Q'_{d_2,d_1}. As they have the same evaluation at P^2, these polynomials are in the same class in $S/I(P^2)$. This also implies that this class is in $S_{d_1}/I(P^2) \cap S_{d_2}/I(P^2)$ and Q_{d_1,d_2} satisfies the conditions in the statement. □

Example E.3.8. We continue with Example E.3.6. We had $q = 4 \leq d_1 < d_2 = 5$. Thus, by Lemma E.3.7, we have the polynomials $Q_{4,5}$ and $Q'_{5,4}$ from (E.3.8) in $S_4/I(P^2) \cap S_5/I(P^2)$:

$$\begin{aligned} Q_{4,5} &= x_2^4 + x_1^2x_2^2 + x_0^2x_2^2 + x_0^2x_1x_2, \\ Q'_{5,4} &= x_2^5 + x_1^4x_2 + x_0^4x_2 + x_0x_1^2x_2^2. \end{aligned}$$

It is easy to check that both polynomials have the same evaluation at $[\{1\} \times \mathbb{F}_4^2]$ as $x_2 + x_2^2 + x_1x_2 + x_1^2x_2^2$, the same evaluation at $[\{0\} \times \{1\} \times \mathbb{F}_4]$ as $x_2 + x_2^2$, and both evaluate to 1 at $[0:0:1]$. Therefore, they have the same evaluation at P^2.

With the notation as above, we present the main result of this section.

Theorem E.3.9. *Let $1 \leq d_1 < d_2 \leq 2(q-1)$, and let $Y = \{0, 1, \ldots, \min\{d_1-1, d_2-q\}\}$. If $d_1 \equiv d_2 \bmod q-1$, A^{d_1} is a basis for $S_{d_1}/I(P^2) \cap S_{d_2}/I(P^2)$. If $d_1 \not\equiv d_2 \bmod q-1$, the following set B is a basis for $S_{d_1}/I(P^2) \cap S_{d_2}/I(P^2)$:*

$$B = \begin{cases} A_1^{d_1} & \text{if } d_2 \leq q-1, \\ A_1^{d_1} \cup \left(\bigcup_{a_2 \in Y}\{x_1^{d_1-a_2}x_2^{a_2}\}\right) & \text{if } d_1 \leq q-1 < d_2, \\ A_1^{d_1} \cup \left(\bigcup_{a_2 \in Y}\{x_1^{d_1-a_2}x_2^{a_2}\}\right) \cup \{Q_{d_1,d_2}\} & \text{if } q \leq d_1, \end{cases}$$

with Q_{d_1,d_2} defined as in (E.3.8). In particular, the image by the evaluation map of B is a basis for $\mathrm{PRM}_{d_1}(2) \cap \mathrm{PRM}_{d_2}(2)$.

Proof. The case $d_1 \equiv d_2 \bmod q-1$ is covered by Lemma E.3.1. We assume $d_1 \not\equiv d_2 \bmod q-1$ now. First, we are going to see that the set $A_1^{d_1} \cup \left(\bigcup_{a_2 \in Y}\{x_1^{d_1-a_2}x_2^{a_2}\}\right) \cup \{Q_{d_1,d_2}\}$ is linearly independent in $S/I(P^2)$, which proves that all the sets we are considering are

linearly independent. $A_1^{d_1} \cup \left(\bigcup_{a_2 \in Y} \{x_1^{d_1-a_2} x_2^{a_2}\}\right)$ is linearly independent because it is a subset of A^{d_1}, which is linearly independent. And, when we consider the union with $\{Q_{d_1,d_2}\}$, we preserve linear independence because Q_{d_1,d_2} is the only polynomial of this union that has nonzero evaluation in $[0 : 0 : 1]$, which implies that its evaluation is linearly independent from the rest. On the other hand, these sets are clearly contained in $S_{d_1}/I(P^2)$, and the proofs from Lemmas E.3.3, E.3.5 and E.3.7 show that these sets are also contained in $S_{d_2}/I(P^2)$.

Hence, we only need to prove that B is a system of generators for $S_{d_1}/I(P^2) \cap S_{d_2}/I(P^2)$. Let $f \in S_{d_1}/I(P^2) \cap S_{d_2}/I(P^2)$. If $f(0,0,1) = \lambda \neq 0$, then f has $x_2^{d_1}$ in its support when expressed in terms of the monomials in A^{d_1}. By Lemma E.3.7, we must have $q \leq d_1$. Moreover, we can subtract $\lambda Q_{d_1,d_2}$ from f and obtain a polynomial $f^{(1)}$ such that $f^{(1)}(0,0,1) = 0$, its expression in terms of the monomials in A^{d_1} only contains monomials from $A_1^{d_1} \cup A_2^{d_1}$, and $f^{(1)} \in S_{d_1}/I(P^2) \cap S_{d_2}/I(P^2)$. On the other hand, if $f^{(1)}$ has monomials from $A_1^{d_1}$ in its support when expressed in terms of the monomials in A^{d_1}, by Lemma E.3.3 we know that we can subtract adequate multiples of those monomials and obtain a polynomial $f^{(2)} \in S_{d_1}/I(P^2) \cap S_{d_2}/I(P^2)$ that only has monomials from $A_2^{d_1}$ in its support. Finally, we can apply Lemma E.3.5 to $f^{(2)}$ and obtain that $f^{(2)}$ can be generated by $\bigcup_{a_2 \in Y} \{x_1^{d_1-a_2} x_2^{a_2}\}$. If $f(0,0,1) = 0$, we can apply the reasoning we have used above for $f^{(1)}$. □

Note that the basis from the previous result is formed by monomials, except when $q \leq d_1$, where we consider Q_{d_1,d_2}. This polynomial cannot be reduced to a monomial subtracting other monomials from the basis B of Theorem E.3.9 because both $x_2^{d_1}$ and $x_1^{d_1-\overline{d_2}} x_2^{\overline{d_2}}$ are linearly independent from the rest of monomials from B by Lemma E.2.7 (also check the definition of Y from Lemma E.3.5 and note that $d_2 - q < \overline{d_2}$).

Example E.3.10. Continuing with Examples E.3.4, E.3.6 and E.3.8, we see that the set

$$A_1^4 \cup \{x_1^4, x_1^3 x_2\} \cup \{x_2^4 + x_1^2 x_2^2 + x_0^2 x_2^2 + x_0^2 x_1 x_2\}$$

is a basis for $S_4/I(P^2) \cap S_5/I(P^2)$.

By counting the elements of the set B in Theorem E.3.9, we obtain the dimension of $S_{d_1}/I(P^2) \cap S_{d_2}/I(P^2)$.

Corollary E.3.11. *Let* $1 \leq d_1 < d_2 \leq 2(q-1)$. *Let* $k_1 = \dim \mathrm{RM}_{d_1-1}(2)$. *If* $d_1 \equiv d_2 \bmod q-1$, *then* $\dim(\mathrm{PRM}_{d_1}(2) \cap \mathrm{PRM}_{d_2}(2)) = \dim \mathrm{PRM}_{d_1}(2)$. *If* $d_1 \not\equiv d_2 \bmod q-1$, *then*

$$\dim(\mathrm{PRM}_{d_1}(2) \cap \mathrm{PRM}_{d_2}(2)) = \begin{cases} k_1 & \text{if } d_2 \leq q-1, \\ k_1 + \min\{d_1, d_2 - (q-1)\} & \text{if } d_1 \leq q-1 < d_2, \\ k_1 + d_2 - q + 2 & \text{if } q \leq d_1. \end{cases}$$

In the case where $d_2 = d_1^\perp = 2(q-1) - d_1$, Corollary E.3.11 simplies to the following.

Corollary E.3.12. *Let* $1 \leq d \leq q-1$, *let* $Y = \{0, 1, \ldots, \min\{d-1, q-d-2\}\}$, *and let* $k_1 = \dim \mathrm{RM}_{d-1}(2)$. *If* $2d \equiv 0 \bmod q-1$, *then* $\mathrm{PRM}_d(2) \cap \mathrm{PRM}_d^\perp(2) = \mathrm{PRM}_d(2)$. *If* $2d \not\equiv 0 \bmod q-1$, *a basis for* $\mathrm{PRM}_d(2) \cap \mathrm{PRM}_d^\perp(2)$ *is given by* $A_1^d \cup \left(\bigcup_{a_2 \in Y} \{x_1^{d-a_2} x_2^{a_2}\}\right)$. *Consequently,* $\dim \mathrm{PRM}_d(2) \cap \mathrm{PRM}_d^\perp(2) = k_1 + \min\{d, q-d-1\}$.

Proof. For the case $d = q - 1$, we have that $\mathrm{PRM}_{q-1}(2) = \mathrm{PRM}_{q-1}(2) \cap \mathrm{PRM}^{\perp}_{q-1}(2)$ by Theorem E.2.2. For $1 \leq d < q-1$, from Theorem E.2.2 we see that $\mathrm{PRM}^{\perp}_{d}(2) = \mathrm{PRM}_{d^{\perp}}(2)$, with $d^{\perp} = 2(q-1)-d$. The result is obtained by applying the previous results with $d_1 = d$, $d_2 = d^{\perp}$. □

Note that for $q \leq d < 2(q-1)$, we can also obtain the dimension of the hull by considering $\mathrm{PRM}_{d^{\perp}}(2)$ in the previous result. For $d = 2(q-1)$, by Theorem E.2.2 the dual code is generated by the evaluation of 1, and by Lemma E.3.2 we obtain $\mathrm{PRM}_{2(q-1)}(2) \cap \mathrm{PRM}^{\perp}_{2(q-1)}(2) = \{0\}$.

E.3.2 Hermitian hull

In the Hermitian case, we consider codes defined over $\mathbb{F}^n_{q^2}$, and the Hermitian product of two vectors $v, w \in \mathbb{F}^n_{q^2}$ is

$$v \cdot_h w = \sum_{i=1}^{n} v_i w_i^q.$$

The Hermitian dual of a code $C \subset \mathbb{F}^n_{q^2}$ is defined as $C^{\perp_h} := \{v \in \mathbb{F}^n_{q^2} \mid v \cdot_h w = 0, \ \forall\, w \in C\}$. We recall that we defined the Hermitian hull as $\mathrm{Hull}^H(C) = C \cap C^{\perp_h}$. It is easy to check that, for a code $C \subset \mathbb{F}^n_{q^2}$, we have that $C^{\perp_h} = (C^{\perp})^q$, where we consider the component wise power of q. In particular, this implies that the Hermitian dual and the Euclidean dual have the same parameters. In this section we show that we may apply similar techniques to the ones used in the previous section to compute the Hermitian hull in some cases. In what follows, as we are working over $\mathbb{F}_{q^2}$, we change q by q^2 in the definitions of S, A^d_i, for $i = 1, 2, 3$, etc. We show now how the main definitions from the other sections are adapted to the Hermitian case in this section:

1. $S = \mathbb{F}_{q^2}[x_0, x_1, x_2]$.
2. Projective and affine Reed-Muller codes are defined for $1 \leq d \leq m(q^2 - 1)$.
3. A^d is defined for $1 \leq d \leq 2(q^2 - 1)$. If we have $x_0^{a_0} x_1^{a_1} x_2^{a_2} \in A^d_1$, then $0 \leq a_1, a_2 \leq q^2 - 1$, and if $x_0^{a_0} x_1^{a_1} x_2^{a_2} \in A^d_2$, then $0 \leq a_2 \leq q^2 - 1$. For Lemma E.2.9, we have $0 \leq a_i \leq q^2 - 1$, for $1 \leq i \leq 2$.
4. Now $\overline{z}$ is the integer $1 \leq \overline{z} \leq q^2 - 1$ such that $\overline{z} \equiv z \bmod q^2 - 1$ when $z > 0$, and $\overline{z} = 0$ otherwise.

In the affine case, Reed-Muller codes are either contained in their Euclidean dual or they contain it, which means that the computation of the Euclidean hull is trivial. However, the following result from [12] remarks that computing the Hermitian hull is more difficult than computing the Euclidean hull in the affine case.

Proposition E.3.13. *The codes' inclusion* $\mathrm{RM}_d(q^2, m) \subset \mathrm{RM}^{\perp_h}_d(q^2, m)$ *holds if, and only if,* $0 \leq d \leq m(q-1) - 1$.

Moreover, it is not hard to obtain a basis for the intersection of a Reed-Muller code with the Hermitian dual of another Reed-Muller code.

Definition E.3.14. Let $0 \leq d_1, d_2 \leq m(q^2-1)$. We define

$$U_{d_1,d_2} := \{x_1^{a_1}x_2^{a_2} \mid 0 \leq a_1, a_2 \leq q^2-1,\ a_1+a_2 \leq d_1,\ \overline{qa_1}+\overline{qa_2} \leq 2(q^2-1)-d_2-1\}.$$

Proposition E.3.15. *The image by the evaluation map over $\mathbb{A}^2$ of U_{d_1,d_2} is a basis for $\mathrm{RM}_{d_1}(q^2,2) \cap \mathrm{RM}_{d_2}^{\perp_h}(q^2,2)$.*

Proof. The monomials $x_1^{a_1}x_2^{a_2}$ with $0 \leq a_1, a_2 \leq q^2-1$ have linearly independent evaluations over $\mathbb{A}^2$, and their evaluations generate $\mathbb{F}_{q^2}^{q^4}$ (the full code). The evaluation of a monomial $x_1^{a_1}x_2^{a_2}$ with $0 \leq a_1, a_2 \leq q^2-1$ and $a_1+a_2 \leq d_1$ is in $\mathrm{RM}_{d_2}^{\perp_h}(q^2,2)$ if and only if $x_1^{a_1}x_2^{a_2} \equiv (x_1^{b_1}x_2^{b_2})^q \bmod I(\mathbb{A}^2)$ for some $0 \leq b_1, b_2 \leq q^2-1$ such that $b_1+b_2 \leq 2(q^2-1)-d_2-1$, where $I(\mathbb{A}^2) = \langle x_1^{q^2}-x_1, x_2^{q^2}-x_2\rangle$ (we have used the duality from Theorem E.2.5 and the fact that $\mathrm{RM}_{d_2}^{\perp_h}(q^2,2) = (\mathrm{RM}_{d_2}^{\perp}(q^2,2))^q$). If $a_i \neq 0$ for some $i=1,2$, then $x_1^{a_1}x_2^{a_2} \equiv (x_1^{b_1}x_2^{b_2})^q \bmod I(\mathbb{A}^2)$ implies $a_i \equiv qb_i \bmod q^2-1$ with $b_i \neq 0$, which is equivalent to having $b_i = \overline{qa_i}$ (recall Remark E.2.11). If $a_i = 0$ for some $i=1,2$, then $x_1^{a_1}x_2^{a_2} \equiv (x_1^{b_1}x_2^{b_2})^q \bmod I(\mathbb{A}^2)$ implies $b_i = 0 = \overline{qa_i}$ in this case as well. Therefore, in both cases $b_i = \overline{qa_i}$, which finishes the proof. □

Remark E.3.16. The previous result can be extended in the obvious way to the Reed-Muller codes in m variables. For the Hermitian hull of affine Reed-Muller codes we only need to consider $U_{d,d}$, but for projective Reed-Muller codes we will also consider $U_{d-1,d}$, and that is why we expressed Proposition E.3.15 in full generality with two degrees d_1 and d_2.

Using that $C^{\perp_h} = (C^{\perp})^q$, if we consider $(A_i^d)^q := \{(x^\alpha)^q \mid x^\alpha \in A_i^d\}$ and $d^\perp = 2(q^2-1)-d$, we have that the image by the evaluation map of $(A^{d^\perp})^q := \bigcup_{i=1}^3 (A_i^{d^\perp})^q$ is a basis for $\mathrm{PRM}_d^{\perp_h}(q^2,2) = (\mathrm{PRM}_{d^\perp}(q^2,2))^q$ (if $d \not\equiv 0 \bmod q^2-1$). Following the notation from the previous section, we will denote by $S_{d^\perp}^q/I(P^2)$ the vector space generated in $S/I(P^2)$ by $\bigcup_{i=1}^3 (A_i^{d^\perp})^q$.

To compute the dimension of the Hermitian hull of projective Reed-Muller codes it is enough to consider the case with $d \leq q^2-1$. This is because if we assume $d > q^2-1$, then

$$\mathrm{PRM}_d(q^2,2) \cap \mathrm{PRM}_{d^\perp}^q(q^2,2) = (\mathrm{PRM}_d^q(q^2,2) \cap \mathrm{PRM}_{d^\perp}(q^2,2))^q,$$

and then at the right-hand side of the previous equality we have the Hermitian hull of a projective Reed-Muller code of degree $d^\perp < q^2-1$, to the power of q. Moreover, because of Theorem E.2.2 we are going to avoid the case with $d = q^2-1$ when giving results for the Hermitian hull (for results about $S_d/I(P^2) \cap S_{d^\perp}^q/I(P^2)$ we will still consider $d = q^2-1$). This is because in that case $\mathrm{PRM}_d^{\perp}(q^2,2) = \mathrm{PRM}_{d^\perp}(q^2,2) + \langle(1,\ldots,1)\rangle \neq \mathrm{PRM}_{d^\perp}(q^2,2)$, and $\mathrm{PRM}_d^{\perp_h}(q^2,2) = (\mathrm{PRM}_{d^\perp}(q^2,2)+\langle(1,\ldots,1)\rangle)^q \neq \mathrm{PRM}_{d^\perp}^q(q^2,2) \cong S_{d^\perp}^q/I(P^2)$. Hence, if $d = q^2-1$ we do not have the isomorphism between $\mathrm{PRM}_d^{\perp_h}(q^2,2)$ and $S_{d^\perp}^q/I(P^2)$, and also this case is the least interesting for quantum codes because we do not have a bound for the minimum distance of the dual code.

As a consequence of Proposition E.3.13 and Proposition E.3.15, we have the following result.

Lemma E.3.17. *Let $1 \leq d \leq q^2-1$ and let $U := \{x_0^{d-a_1-a_2}x_1^{a_1}x_2^{a_2} \mid x_1^{a_1}x_2^{a_2} \in U_{d-1,d}\} \subset S_d$. Then, the classes of the monomials in U are contained in $S^q_{d^\perp}/I(P^2)$. Moreover, if $d \leq 2(q-1)$, $U = A_1^d$.*

Proof. Let $1 \leq d \leq q^2-1$, and let $x_0^{a_0}x_1^{a_1}x_2^{a_2} \in U$. By definition, it is clear that $x_0^{a_0}x_1^{a_1}x_2^{a_2} \in S^q_{d^\perp}/I(P^2)$ because $x_0^{a_0}x_1^{a_1}x_2^{a_2} \equiv (x_0^{d^\perp-\overline{qa_1}-\overline{qa_2}}x_1^{\overline{qa_1}}x_2^{\overline{qa_2}})^q \bmod I(P^2)$, where $\overline{qa_1}+\overline{qa_2} \leq d^\perp-1$ by the definition of $U_{d-1,d}$. If $d \leq 2(q-1)$, we consider $x_0^{a_0}x_1^{a_2}x_2^{a_2} \in A_1^d$. Therefore, $a_1+a_2 \leq d-1$ and we have that

$$\overline{qa_1}+\overline{qa_2} \leq qa_1+qa_2 \leq q(d-1) \leq 2(q^2-1)-2(q-1)-q \leq 2(q^2-1)-d-1.$$

This means that $A_1^d \subset U$ in this case, and the other contention always holds. □

Example E.3.18. We consider $q=3$ and $d=7$. Hence, we work over $\mathbb{F}_{3^2}$ and $d > 2(q-1)=4$ in this case. One can check that we have

$$U = A_1^7 \setminus \{x_0x_1x_2^5, x_0x_1^2x_2^4, x_0x_1^4x_2^2, x_0x_1^5x_2, x_0^3x_1^2x_2^2, x_0^4x_1x_2^2, x_0^4x_1^2x_2\},$$

where A_1^7 is formed by all the monomials of degree 7 that are divisible by x_0 in this case. For instance, for the monomial $x_0x_1x_2^5$ we have $a_1=1$, $a_2=5$, and we check

$$\overline{qa_1}+\overline{qa_2} = \overline{3}+\overline{15} = 10 \not\leq 9 = d^\perp,$$

which implies $x_0x_1x_2^5 \notin U$.

Remark E.3.19. To compute the dimension of the hull of projective Reed-Muller codes we will need the size of the set U from Lemma E.3.17. We give a combinatorial formula for $|U|$ in Lemma E.5.1 of the Appendix. Moreover, it is possible to obtain a combinatorial formula for $|U_{d,d}|$ as well, as we note in Remark E.5.2, which gives the dimension of the Hermitian hull for affine Reed-Muller codes in 2 variables.

In the following results we argue in a similar way to Section E.3.1 to show which polynomials can be in $S_d/I(P^2) \cap S^q_{d^\perp}/I(P^2)$ depending on whether the monomials in the support of these polynomials are contained in A_2^d or if they have x_2^d in their support (we recall that $A_3^d = \{x_2^d\}$). We restrict to the case $1 \leq d \leq 2(q-1)$ in some results because in that case we have $U = A_1^d$ by Lemma E.3.17, which is similar to what happens in the Euclidean case. For the following results, recall that $\overline{z}$ is a representative of the class of z modulo q^2-1.

Lemma E.3.20. *Let $1 \leq d \leq 2(q-1)$. Let $f \in S_d$ such that it only has monomials from A_2^d in its support, i.e., it can be expressed as*

$$f = \sum_{a_1+a_2=d, 0<a_1, 0\leq a_2\leq q^2-1} \lambda_{a_1,a_2}x_1^{a_1}x_2^{a_2}, \lambda_{a_1,a_2} \in \mathbb{F}_{q^2}.$$

Let $T = \{a_2 \mid a_2 < d,\ d^\perp > \overline{qa_2}+(q^2-1)\}$ and $T_f = \{0 \leq a_2 \leq q-1 \mid \lambda_{d-a_2,a_2} \neq 0\}$. Then $f \in S^q_{d^\perp}/I(P^2)$ if and only if $d \equiv 0 \bmod q-1$ or $T_f \subset T$.

Proof. Assuming that $f \in S^q_{d^\perp}/I(P^2)$, there is an expression

$$f \equiv \sum_{(x_0^{\alpha_0}x_1^{\alpha_1}x_2^{\alpha_2})^q \in (A^{d^\perp})^q} \mu_{\alpha_0,\alpha_1,\alpha_2}(x_0^{\alpha_0}x_1^{\alpha_1}x_2^{\alpha_2})^q \bmod I(P^2), \mu_{\alpha_0,\alpha_1,\alpha_2} \in \mathbb{F}_{q^2}. \tag{E.3.9}$$

We have $f(0,0,1) = 0$, which means that $\mu_{0,0,d^\perp} = 0$. Following the proof of Lemma E.3.5, we consider $\mathrm{in}(f) = x_1^{a_1}x_2^{a_2}$, with $a_1 > 0$, $0 \le a_2 \le q^2-1$ and $a_1+a_2 = d$ (since $d \le 2(q-1)$, we also have $a_1 \le q^2-1$). Because of (E.3.9) we must have some monomial in $(A^{d^\perp})^q$ such that its expression in the basis from Lemma E.2.9 contains $x_1^{a_1}x_2^{a_2}$ in its support. Let $\gamma_i = \overline{qa_i}$, for $i = 1, 2$, which implies that $q\gamma_i \equiv a_i \bmod q^2-1$. The only monomials in $(A^{d^\perp})^q$ that contain $x_1^{a_1}x_2^{a_2}$ in their expression in terms of the basis from Lemma E.2.9 are $(x_1^{d^\perp-\gamma_2}x_2^{\gamma_2})^q$ if $q(d^\perp-\gamma_2) \equiv a_1 \bmod q^2-1$, and $(x_0^{\gamma_0}x_1^{\gamma_1}x_2^{\gamma_2})^q$ if $\gamma_0 = d^\perp-\gamma_1-\gamma_2 > 0$.

In the first case, $q(d^\perp-\gamma_2) \equiv a_1 \bmod q^2-1$ implies that $qd^\perp \equiv d \bmod q^2-1$, which happens if and only if $d \equiv 0 \bmod q-1$. Taking into account that $d \le 2(q-1)$, we have $d^\perp > q^2-1 \ge \gamma_2$, and we have $x_1^{a_1}x_2^{a_2} \equiv (x_1^{d^\perp-\gamma_2}x_2^{\gamma_2})^q \bmod I(P^2)$. Moreover, in this situation we can do this for all the monomials from A_2^d in the support of f.

If $d \not\equiv 0 \bmod q-1$, the only monomial in $(A^{d^\perp})^q$ with $x_1^{a_1}x_2^{a_2}$ in its expression in terms of the elements of the basis from Lemma E.2.9 is $(x_0^{\gamma_0}x_1^{\gamma_1}x_2^{\gamma_2})^q$ with $\gamma_0 = d^\perp-\gamma_1-\gamma_2$, if $d^\perp-\gamma_1-\gamma_2 > 0$. This is because, by Lemma E.2.12, we have that

$$(x_0^{\gamma_0}x_1^{\gamma_1}x_2^{\gamma_2})^q \equiv x_1^{a_1}x_2^{a_2} + (x_0-1)(x_2^{a_2}+x_1-1) \bmod I(P^2),$$

if $\gamma_0 > 0$. Hence, we must have $\mu_{\gamma_0,\gamma_1,\gamma_2} = \lambda_{a_1,a_2}$. If we denote by $((A^{d^\perp})^q)^{(1)} = (A^{d^\perp})^q \setminus \{(x_0^{\gamma_0}x_1^{\gamma_1}x_2^{\gamma_2})^q\}$, we obtain

$$\begin{aligned} f^{(1)} =& f - \lambda_{a_1,a_2}x_1^{a_1}x_2^{a_2} \\ \equiv& \sum_{(x_0^{\alpha_0}x_1^{\alpha_1}x_2^{\alpha_2})^q \in ((A^{d^\perp})^q)^{(1)}} \mu_{\alpha_0,\alpha_1,\alpha_2}(x_0^{\alpha_0}x_1^{\alpha_1}x_2^{\alpha_2})^q \\ &+ \mu_{d^\perp-\overline{qa_1}-\overline{qa_2},\overline{qa_1},\overline{qa_2}}(x_0-1)(x_2^{a_2}+x_1-1) \bmod I(P^2). \end{aligned} \tag{E.3.10}$$

Arguing as in the proof of Lemma E.3.5, after l steps we get

$$\begin{aligned} 0 \equiv& \sum_{(x_0^{\alpha_0}x_1^{\alpha_1}x_2^{\alpha_2})^q \in ((A^{d^\perp})^q)^{(l)}} \mu_{\alpha_0,\alpha_1,\alpha_2}(x_0^{\alpha_0}x_1^{\alpha_1}x_2^{\alpha_2})^q \\ &+ (x_0-1)\sum_{a_2 \in T_f} \mu_{d^\perp-\overline{q(d-a_2)}-\overline{qa_2},\overline{q(d-a_2)},\overline{qa_2}}(x_2^{a_2}+x_1-1) \bmod I(P^2), \end{aligned} \tag{E.3.11}$$

where $T_f = \{0 \le a_2 \le q^2-1 \mid \lambda_{d-a_2,a_2} \ne 0\}$. With this notation, we have that $((A^{d^\perp})^q)^{(l)} = (A^{d^\perp})^q \setminus \bigcup_{a_2 \in T}\{(x_0^{\gamma_0}x_1^{\gamma_1}x_2^{\gamma_2})^q, \gamma_0 = d^\perp-\gamma_1-\gamma_2,\ \gamma_1 = \overline{q(d-a_2)},\ \gamma_2 = \overline{qa_2}\}$.

If we express all the monomials in (E.3.11) in terms of the basis from Lemma E.2.9, then we must have the coefficient of each element of the basis equal to 0. The monomials from (E.3.11) in the second sum are already expressed in terms of the basis from Lemma E.2.9. If we focus on the monomial $x_2^{a_2}$ for some $a_2 \in T_f$ with $a_2 > 0$, we see that all the monomials $(x_0^{c_0}x_1^{c_1}x_2^{\gamma_2})^q \in ((A^{d^\perp})^q)^{(l)}$ with $0 < c_0$, $0 < c_1 \le q^2-1$, $qc_1 \not\equiv d-a_2 \bmod q^2-1$, and $c_0+c_1+\gamma_2 = d^\perp$, have $x_2^{a_2}$ in their expression in terms of the basis from Lemma E.2.9:

$$(x_0^{c_0}x_1^{c_1}x_2^{\gamma_2})^q \equiv x_1^{\overline{qc_1}}x_2^{a_2} + (x_0-1)(x_2^{a_2}+x_1-1) \bmod I(P^2).$$

In fact, these are the only monomials from $((A^{d^\perp})^q)^{(l)}$ with $x_2^{a_2}$ in their expression (the one with $qc_1 \equiv d-a_2 \bmod q^2-1$ is not contained in $((A^{d^\perp})^q)^{(l)}$). However, if we have $\mu_{c_0,c_1,\gamma_2} \neq 0$, some other monomial from $((A^{d^\perp})^q)^{(l)}$ must cancel the monomial $x_1^{\overline{qc_1}}x_2^{a_2}$ from (E.3.11). The only other monomial in $((A^{d^\perp})^q)^{(l)}$ with $x_1^{\overline{qc_1}}x_2^{a_2}$ in its support when expressed in terms of the basis from Lemma E.2.9 is $(x_1^{c_1+q^2-1}x_2^{\gamma_2})^q$ (we cannot use $(x_1^{c_1}x_2^{\gamma_2})^q$ because $c_1+\gamma_2 < d^\perp$), if $c_1+\gamma_2+q^2-1 = d^\perp$ (which implies $c_0 = q^2-1$). In our case, we always have $q^2-1 < d^\perp$, but still we must also have $d^\perp > \gamma_2+q^2-1$ to ensure $c_1 > 0$.

Therefore, if $d^\perp - \gamma_2 - (q^2-1) = c_1 > 0$, we can consider the following polynomial in $S^q_{d^\perp}/I(P^2)$:

$$(x_0^{q^2-1}x_1^{c_1}x_2^{\gamma_2})^q - (x_1^{c_1+q^2-1}x_2^{\gamma_2})^q \equiv (x_0-1)(x_2^{a_2}+x_1-1) \bmod I(P^2).$$

For every $a_2 \in T_f$, we must have $\mu_{q^2-1,c_1,\gamma_2} = -\mu_{0,c_1+q^2-1,\gamma_2} = \lambda_{d-a_2,a_2}$ to cancel the polynomial $(x_0-1)(x_2^{a_2}+x_1-1)$ from (E.3.3). Thus, have seen that $d^\perp > \gamma_2+(q^2-1)$, which implies that $T_f \subset T$.

These are necessary conditions, and now we show that they are sufficient. We assume $T_f \subset T$, and for each $a_2 \in T_f$, we denote $\gamma_1 = \overline{q(d-a_2)}$ as before. Then we have

$$x_1^{d-a_2}x_2^{a_2} \equiv (x_1^{d^\perp-\gamma_2}x_2^{\gamma_2} - x_0^{q^2-1}x_1^{\overline{d^\perp}-\gamma_2}x_2^{\gamma_2} + x_0^{d^\perp-\gamma_1-\gamma_2}x_1^{\gamma_1}x_2^{\gamma_2})^q \bmod I(P^2). \quad \text{(E.3.12)}$$

We note that if $\overline{d^\perp} = d^\perp-(q^2-1) > \gamma_2$, then $d^\perp > \gamma_1+\gamma_2$. The previous equality is easy to check because both sides have the same evaluation at $P^2 = [\{1\}\times\mathbb{F}_{q^2}^2] \cup [\{0\}\times\{1\}\times\mathbb{F}_{q^2}] \cup \{[0:0:1]\}$. Hence, $x_1^{d-a_2}x_2^{a_2} \in S_d/I(P^2) \cap S^q_{d^\perp}/I(P^2)$ for each $a_2 \in T_f$, which implies that $f \in S_d/I(P^2) \cap S^q_{d^\perp}/I(P^2)$. □

Lemma E.3.21. *Let $1 \le d \le 2(q-1)$. There is some $f \in S_d$ with x_2^d in its support and such that $f \in S^q_{d^\perp}/I(P^2)$ if and only if $d \equiv 0 \bmod q-1$.*

Proof. If $d \equiv 0 \bmod q-1$, then we have $x_2^d \equiv x_2^{qd^\perp} \bmod I(P^2)$ because

$$d \equiv qd^\perp \bmod q^2-1 \iff (q+1)d \equiv 0 \bmod q^2-1 \iff d \equiv 0 \bmod q-1.$$

Therefore, we only have to prove the other implication.

Let $f \in S_d$. By Lemma E.3.17, we can assume that the support of f is contained in $(A_2^{d^\perp})^q \cup (A_3^{d^\perp})^q$, i.e., it can be expressed as

$$f = \sum_{a_1+a_2=d, 0<a_1, 0\le a_2\le q^2-1} \lambda_{a_1,a_2}x_1^{a_1}x_2^{a_2} + \lambda_{0,d}x_2^d, \lambda_{a_1,a_2} \in \mathbb{F}_{q^2}.$$

We assume that $\lambda_{0,d} \neq 0$. As in the previous result, we must have an expression

$$f \equiv \sum_{x_0^{a_0}x_1^{a_1}x_2^{a_2} \in (A^{d^\perp})^q} \mu_{a_0,a_1,a_2}x_0^{a_0}x_1^{a_1}x_2^{a_2} \bmod I(P^2), \mu_{a_0,a_1,a_2} \in \mathbb{F}_{q^2}. \quad \text{(E.3.13)}$$

The only monomials in $(A^{d^\perp})^q$ with x_2^d in their expression in terms of the basis from Lemma E.2.9 are $(x_0^{\beta_0}x_1^{\beta_1}x_2^{\beta_2})^q$, for some $0 < \beta_0$, $0 < \beta_1 \le q^2-1$, $0 < \beta_2 \le q^2-1$, such that $\beta_0+\beta_1+\beta_2 = d^\perp$ and $q\beta_2 \equiv d \bmod q^2-1$; and x_2^d if $d \equiv 0 \bmod q^2-1$. We assume

now that $d \not\equiv 0 \bmod q^2-1$, and we will arrive at a contradiction. Thus, we focus on the first type of monomials, which by Lemma E.2.12 can be expressed as

$$(x_0^{\beta_0}x_1^{\beta_1}x_2^{\beta_2})^q \equiv x_1^{\overline{q\beta_1}}x_2^d + (x_0-1)(x_2^d+x_1-1) \bmod I(P^2). \tag{E.3.14}$$

The monomials $x_1^{\overline{q\beta_1}}x_2^d$ have degree greater than d. Thus, they cannot be in the support of f and they have to be cancelled in the expression from (E.3.13) if we consider some monomial $(x_0^{\beta_0}x_1^{\beta_1}x_2^{\beta_2})^q$. The only other monomial in $(A^{d^\perp})^q$ with $x_1^{\overline{q\beta_1}}x_2^d$ in its expression from the basis from Lemma E.2.9 is $(x_1^{\beta_1+q^2-1}x_2^{\beta_2})^q$ if $d^\perp = \beta_1+\beta_2+q^2-1$, which implies $\beta_0 = q^2-1$ and $\beta_1 = d^\perp-\beta_2-(q^2-1)$. Thus, there is only one monomial in $(A^{d^\perp})^q$ that we can consider, and we have

$$x_2^d \equiv (x_1^{\beta_1+q^2-1}x_2^{\beta_2})^q - (x_0^{\beta_0}x_1^{\beta_1}x_2^{\beta_2})^q + (x_0-1)(x_1-1) + x_0x_2^d \bmod I(P^2).$$

Similarly to the proof of Lemma E.3.5, we must have $-\mu_{\beta_0,\beta_1,\beta_2} = \mu_{0,\beta_1+q^2-1,\beta_2} = \lambda_{0,d}$. We can define in this case $((A_2^{d^\perp})^q)^{(1)} = (A_2^{d^\perp})^q \setminus \{(x_0^{\beta_1}x_1^{\beta_1}x_2^{\beta_2})^q, (x_1^{\beta_1+q^2-1}x_2^{\beta_2})^q\}$, and consider

$$\begin{aligned} f^{(1)} =& f - \lambda_{0,d}x_2^d \\ \equiv& \sum_{x_0^{a_0}x_1^{a_1}x_2^{a_2} \in ((A^{d^\perp})^q)^{(1)}} \mu_{a_0,a_1,a_2}x_0^{a_0}x_1^{a_1}x_2^{a_2} - \lambda_{0,d}\left((x_0-1)(x_1-1)+x_0x_2^d\right) \bmod I(P^2). \end{aligned} \tag{E.3.15}$$

Arguing as in Lemma E.3.5 and using Lemma E.3.17, we obtain that there must be a sum of monomials in $((A^{d^\perp})^q)^{(l)}$ equal to $\lambda_{0,d}\left((x_0-1)(x_1-1)+x_0x_2^d\right)$. This implies that we have the evaluation of $(x_0-1)(x_1-1)+x_0x_2^d$ in $\mathrm{PRM}_d^{\perp_h}(q^2,2)$. This is a contradiction because we have the evaluation of $(x_0^{d^\perp-\beta_2}x_2^{\beta_2})^q$ in $\mathrm{PRM}_d^{\perp_h}(q^2,2)$, and $(x_0-1)(x_1-1)+x_0x_2^d-(x_0^{d^\perp-\beta_2}x_2^{\beta_2})^q \equiv (x_0-1)(x_1-1) \bmod I(P^2)$, whose evaluation has Hamming weight 1. □

Let $1 \le d \le q^2-1$. In the next result we give a basis of $S_d/I(P^2) \cap S_{d^\perp}^q/I(P^2)$ for $1 \le d \le 2(q-1)$ using the previous results, and we give a linearly independent set contained in $S_d/I(P^2) \cap S_{d^\perp}^q/I(P^2)$ for the case $2(q-1) < d \le q^2-1$.

To state the next result, we use the following sets of polynomials. We recall that $U = \{x_0^{d-a_1-a_2}x_1^{a_1}x_2^{a_2} \mid x_1^{a_1}x_2^{a_2} \in U_{d-1,d}\}$, where we consider $U_{d-1,d}$ as in Definition E.3.14. We define

$$V := \{x_1^{d-a_2}x_2^{a_2} \mid a_2 \in T\},$$

where T is defined as in Lemma E.3.20. Finally, for the case $2(q-1) < d \le q^2-1$ we define

$$\begin{aligned} W := \{x_1^{d-a_2}x_2^{a_2} + x_0^{d-\overline{qd^\perp-a_2}-a_2}x_1^{\overline{qd^\perp-a_2}}x_2^{a_2} \mid & q^2-1 \ge d^\perp - \overline{qa_2} > \overline{q(d-a_2)} \\ & \text{and } d-a_2 > \overline{qd^\perp-a_2}\}. \end{aligned}$$

We are interested in W because of the following result.

Lemma E.3.22. *We have $W \subset S_d/I(P^2) \cap S_{d^\perp}^q/I(P^2)$, and $U \cup V \cup W$ is a linearly independent set in $S/I(P^2)$.*

Proof. If $d^\perp - \overline{qa_2} > \overline{q(d-a_2)}$ and $d - a_2 > \overline{qd^\perp - a_2}$ (these conditions come from the definition of W), then

$$x_1^{d-a_2}x_2^{a_2} + x_0^{d-\overline{qd^\perp-a_2}-a_2}x_1^{\overline{qd^\perp-a_2}}x_2^{a_2} \equiv (x_1^{d^\perp-\overline{qa_2}}x_2^{\overline{qa_2}} + x_0^{d^\perp-\overline{q(d-a_2)}-\overline{qa_2}}x_1^{\overline{q(d-a_2)}}x_2^{\overline{qa_2}})^q \bmod I(P^2). \tag{E.3.16}$$

This equivalence can be checked by considering the evaluation of both polynomials at P^2. Therefore, we have $W \subset S_d/I(P^2) \cap S^q_{d^\perp}/I(P^2)$. The condition $q^2 - 1 \geq d^\perp - \overline{qa_2}$ ensures $U \cup V \cup W$ is linearly independent. Indeed, both of the monomials in the left hand side of (E.3.16) are monomials from the basis of Lemma E.2.7 and are not in $U \cup V$. The monomial $x_1^{d-a_2}x_2^{a_2}$ from (E.3.16) is not in V because $d^\perp \leq \overline{qa_2} - (q^2-1)$ (see the definition of T in Lemma E.3.20). For the monomial $x_0^{d-\overline{qd^\perp-a_2}-a_2}x_1^{\overline{qd^\perp-a_2}}x_2^{a_2}$, it is not in U because we have $x_1^{\overline{qd^\perp-a_2}}x_2^{a_2} \notin U_{d-1,d}$. To see this, we use the definition of $U_{d-1,d}$ from Definition E.3.14. First, $d - a_2 > \overline{qd^\perp - a_2}$ means that this monomial satisfies the first condition in the definition of $U_{d-1,d}$. For the second one, we would have to check if

$$\overline{q(qd^\perp - a_2)} + \overline{qa_2} = \overline{d^\perp - \overline{qa_2}} + \overline{qa_2} \leq d^\perp - 1. \tag{E.3.17}$$

If $\overline{d^\perp - \overline{qa_2}} < d^\perp - \overline{qa_2}$, we clearly have (E.3.17). However, if $\overline{d^\perp - \overline{qa_2}} = d^\perp - \overline{qa_2}$, we do not have (E.3.17), and this happens if and only if $q^2 - 1 \geq d^\perp - \overline{qa_2}$, which is the condition we are using in the definition of W. □

Now we can state the main result of this section.

Theorem E.3.23. *Let $1 \leq d \leq q^2 - 1$, and $U = \{x_0^{d-a_1-a_2}x_1^{a_1}x_2^{a_2} \mid x_1^{a_1}x_2^{a_2} \in U_{d-1,d}\}$, where we consider $U_{d-1,d}$ as in Definition E.3.14. Let V and W be as in the discussion above. If $d \equiv 0 \bmod q-1$, then $U \cup A_2^d \cup A_3^d$ is a basis for $S_d/I(P^2) \cap S^q_{d^\perp}/I(P^2)$. For $d \not\equiv 0 \bmod q-1$, if $d \leq 2(q-1)$, then $U \cup V = A_1^d \cup V$ is a basis for $S_d/I(P^2) \cap S^q_{d^\perp}/I(P^2)$. Lastly, if $2(q-1) < d \leq q^2 - 1$, then $U \cup V \cup W$ is a linearly independent set contained in $S_d/I(P^2) \cap S^q_{d^\perp}/I(P^2)$.*

Proof. If $d \equiv 0 \bmod q-1$ and $d \leq q^2 - 1$, reasoning as in the proofs of Lemmas E.3.17, E.3.20 and E.3.21, we have $U \cup A_2^d \cup A_3^d$ contained in $S_d/I(P^2) \cap S^q_{d^\perp}/I(P^2)$. Let $f \in S_d$ such that $f \in S^q_{d^\perp}/I(P^2)$ and whose support is contained in $A_1^d \setminus U$. Then f has an expression in terms of the monomials from $(A^{d^\perp})^q$ in $S/I(P^2)$, and this expression only involves the monomials from $(A_1^{d^\perp})^q$. This is because $x_2^{qd^\perp}$ cannot be in the expression because it is nonzero at $[0:0:1]$ while $f(0,0,1) = 0$, and if there were monomials from $(A_2^{d^\perp})^q$, in $[\{0\} \times \{1\} \times \mathbb{F}_{q^2}]$ that expression would have the same evaluation as some polynomial in x_2 with degree less than or equal to $q^2 - 1$, which cannot have q^2 zeroes (f is equal to 0 in those points). We finish this case by using the affine case from Proposition E.3.15.

If $d \not\equiv 0 \bmod q-1$ and $d \leq 2(q-1)$, we have $U = A_1^d$ contained in $S_d/I(P^2) \cap S^q_{d^\perp}/I(P^2)$ by Lemma E.3.17. Arguing as in the proof of Theorem E.3.9 and using Lemma E.3.20 and Lemma E.3.21, we obtain that $U \cup V$ is a basis for $S_d/I(P^2) \cap S^q_{d^\perp}/I(P^2)$.

Finally, in the case $d \not\equiv 0 \bmod q-1$ and $2(q-1) < d < q^2 - 1$, we have from Lemma E.3.17 that U is contained in $S_d/I(P^2) \cap S^q_{d^\perp}/I(P^2)$. The fact that V is contained in $S_d/I(P^2) \cap S^q_{d^\perp}/I(P^2)$ follows from (E.3.12). For W, by Lemma E.3.22, we have that $W \subset S_d/I(P^2) \cap S^q_{d^\perp}/I(P^2)$ and $U \cup V \cup W$ is linearly independent in $S/I(P^2)$. □

From Theorem E.3.23 we can obtain the exact dimension of $S_d/I(P^2) \cap S^q_{d^\perp}/I(P^2)$ if $d \leq 2(q-1)$ or $d \equiv 0 \bmod q-1$. For $2(q-1) < d \leq q^2-1$, $d \not\equiv 0 \bmod q-1$, we only have a lower bound for the dimension of $S_d/I(P^2) \cap S^q_{d^\perp}/I(P^2)$. Note that a lower bound for the dimension of the hull gives an upper bound for the parameter c of the corresponding EAQECC, which is still interesting because it tells us how many maximally entangled pairs are required at most for using that EAQECC. Equivalently, if we use as many maximally entangled pairs as the bound specifies, then we can employ this EAQECC. Nevertheless, in all cases we have checked, this is indeed the true value of the dimension of the hull, which implies that $U \cup V \cup W$ is also a basis for the hull in those cases. In particular, this means that the Hermitian hull is not generated by monomials in general because of W (we saw in the proof of Lemma E.3.22 that no monomial of the polynomials from W is contained in $U \cup V$). We see this in the next example.

Example E.3.24. We continue with the setting from Example E.3.18. We have $d = 7 > 2(q-1)$ and $d \not\equiv 0 \bmod q-1$. Therefore, by Theorem E.3.23, $U \cup V \cup W$ is a linearly independent set contained in $S_d/I(P^2) \cap S^q_{d^\perp}/I(P^2)$. In Example E.3.18 we computed the set U, and we are going to compute the sets V and W now.

For V, we first obtain $T = \{7\}$. This is because $d^\perp - (q^2-1) = 1$ in this case. Thus, $1 > \overline{qa_2}$ implies $a_2 = 0$, and we have $V = \{x_1^7\}$.

Finally, for W, we have to consider $0 \leq a_2 \leq 7$ and check the conditions in the definition of W. In this case, the only a_2 that satisfies the conditions is $a_2 = 1$, and we have $W = \{x_1^6x_2 + x_0^4x_1^2x_2\}$.

It can be checked with Magma [4] that the image by the evaluation map of $U \cup V \cup W$ is, in fact, a basis for the Hermitian hull in this case. We also see that the monomials from the polynomial $x_1^6x_2 + x_0^4x_1^2x_2$ in the set W are not contained in V and U (see Example E.3.18). Hence, we see that in this case the Hermitian hull cannot be generated by monomials from A^d.

We have the following lemma, which gives us the size of the set T (which is the same as the size of the set V as defined prior to Theorem E.3.23) and allows us to give more explicit expressions for the dimension of $S_d/I(P^2) \cap S^q_{d^\perp}/I(P^2)$ in some cases.

Lemma E.3.25. *Let $1 \leq d \leq q^2-1$, and let $d = \beta_0 + \beta_1 q$ be its q-adic expansion. Then*

$$|T| = |V| = \beta_1(q-1-\beta_1) + \min\{\beta_0, q-1-\beta_1\} + \min\{\beta_1, q-1-\beta_0\}.$$

Proof. Let $a_2 \in T$, and we consider its q-adic expansion $a_2 = \alpha_0 + \alpha_1 q$. We must have $a_2 < d$ and $d^\perp > \overline{qa_2} + q^2 - 1$ by the definition of T. It is easy to check that $\alpha_1 + \alpha_0 q$ is the q-adic expansion of $\overline{qa_2}$. The condition $a_2 < d$ translates to the condition

$$\alpha_1 < \beta_1 \text{ or } \alpha_1 = \beta_1 \text{ and } \alpha_0 < \beta_0. \tag{E.3.18}$$

For the other condition, it is easy to check that $q-1-\beta_0 + (q-1-\beta_1)q$ is the q-adic expansion of $d^\perp - (q^2-1) = q^2-1-d$ (using $q^2 = q-1+(q-1)q$). Then, the condition $d^\perp - (q^2-1) > \overline{qa_2}$ translates to

$$\alpha_0 < q-1-\beta_1 \text{ or } \alpha_0 = q-1-\beta_1 \text{ and } \alpha_1 < q-1-\beta_0. \tag{E.3.19}$$

Now we count all the pairs $0 \leq \alpha_0, \alpha_1 \leq q-1$ that satisfy the conditions (E.3.18) and (E.3.19). If $\alpha_0 < q-1-\beta_1$, all the values of α_1 such that $\alpha_1 < \beta_1$ satisfy the conditions. We obtain $\beta_1(q-1-\beta_1)$ pairs in this way.

If $\alpha_0 < q-1-\beta_1$, we also have the possibility of having $\alpha_1 = \beta_1$, but then we must also have $\alpha_0 < \beta_0$ by (E.3.18). Therefore, we obtain the pairs with $\alpha_1 = \beta_1$, and $\alpha_0 = 0, 1, \ldots, \min\{\beta_0 - 1, q-2-\beta_1\}$, i.e., we obtain $\min\{\beta_0, q-1-\beta_1\}$ pairs of this type.

If $\alpha_0 = q-1-\beta_1$, we must have $\alpha_1 < q-1-\beta_0$ by (E.3.19). If we also have $\alpha_1 < \beta_1$, we satisfy (E.3.18) and we obtain $\min\{\beta_1, q-1-\beta_0\}$ pairs. The last option would be to have $\alpha_0 = q-1-\beta_1$ and $\alpha_1 = \beta_1$, in which case we must also have $\alpha_1 = \beta_1 < q-1-\beta_0$ by (E.3.19) and $\alpha_0 = q-1-\beta_1 < \beta_0$ by (E.3.18). But we cannot have $\beta_1 < q-1-\beta_0$ and $q-1-\beta_1 < \beta_0$ simultaneously, which means that this pair does not satisfy the conditions. □

Remark E.3.26. In the previous result, we have that $\beta_1 \leq q-1-\beta_0 \iff \beta_0 \leq q-1-\beta_1 \iff \beta_0+\beta_1 \leq q-1$. Hence, the size of the set T can also be expressed as

$$|T| = \begin{cases} \beta_1(q-1-\beta_1)+\beta_0+\beta_1 & \text{if } \beta_0+\beta_1 \leq q-1, \\ \beta_1(q-1-\beta_1)+2(q-1)-\beta_0-\beta_1 & \text{if } \beta_0+\beta_1 > q-1. \end{cases}$$

Moreover, it is easy to check that these expressions can also be written in the following way:

$$|T| = \begin{cases} d-\beta_1^2 & \text{if } \beta_0+\beta_1 \leq q-1, \\ d-\beta_1^2-2(\beta_0+\beta_1-(q-1)) & \text{if } \beta_0+\beta_1 > q-1. \end{cases}$$

We note that $d \leq 2(q-1) = q+(q-2)$ implies that $\beta_0+\beta_1 \leq q-1$.

Example E.3.27. Continuing with the setting from Example E.3.24, we have that $d = 7 = 1+2\cdot 3$, which means that $\beta_0 = 1$, $\beta_1 = 2$. Thus, by Lemma E.3.25, we obtain

$$|T| = d-\beta_1^2-2(\beta_0+\beta_1-(q-1)) = 1,$$

which is what we obtained in Example E.3.24.

As a consequence of Lemma E.3.17, Theorem E.3.23 and Lemma E.3.25 we have the following result about the dimension of the Hermitian hull. Note that $|V| = |T|$, and $|U|$ is computed in Lemma E.5.1.

Corollary E.3.28. *Let $1 \leq d < q^2-1$, and let $d = \beta_0+\beta_1 q$ be its q-adic expansion. If $d \equiv 0 \bmod q-1$, we have*

$$\dim(\mathrm{PRM}_d(q^2,2) \cap \mathrm{PRM}_d^{\perp_h}(q^2,2)) = \begin{cases} \dim(\mathrm{PRM}_d(q^2,2)) & \text{if } d \leq 2(q-1), \\ |U|+d+1 & \text{if } d > 2(q-1). \end{cases}$$

For the case $d \not\equiv 0 \bmod q-1$: if $d \leq 2(q-1)$, we have

$$\dim(\mathrm{PRM}_d(q^2,2) \cap \mathrm{PRM}_d^{\perp_h}(q^2,2)) = |U|+d-\beta_1^2 = \left|A_1^d\right| + d - \beta_1^2,$$

and if $d > 2(q-1)$, we have the lower bound

$$\dim(\mathrm{PRM}_d(q^2,2) \cap \mathrm{PRM}_d^{\perp_h}(q^2,2)) \geq |U|+|V|+|W|.$$

Example E.3.29. We continue with the setting from Example E.3.24, where we saw that $U \cup V \cup W$ was a basis for the Hermitian hull. Therefore, we have that the dimension of the Hermitian hull is $|U|+|V|+|W|$ (the bound from Corollary E.3.28 is, in fact, the true dimension). From Example E.3.18 we obtain $|U| = 28-7 = 21$, and from Example E.3.24 we obtain $|V| = |W| = 1$. Hence, the dimension of the Hermitian hull in this case is 23.

E.4 Quantum codes from projective Reed-Muller codes

This section is devoted to providing the parameters of the EAQECCs obtained by using projective Reed-Muller codes over the projective plane $\mathbb{P}^2$. Note that, by Theorem E.2.1 and Theorem E.2.2, we know all the parameters of the projective Reed-Muller codes except when $d \equiv 0 \bmod q-1$ (resp. $d \equiv 0 \bmod q^2-1$ in the Hermitian case), in which case we do not know the minimum distance of the dual code. Moreover, in this case the dimension of the hull is not directly given by the computations made in the previous sections because we would have to also consider the constant 1 when computing the intersection $S_{d_1}/I(P^2) \cap S_{d_2}/I(P^2)$ (resp. $S_d/I(P^2) \cap S^q_{d^\perp}/I(P^2)$ in the Hermitian case). Therefore, we avoid this case in the results of this section.

E.4.1 Euclidean EAQECCs

Using the knowledge of the relative hull for two projective Reed-Muller codes, we can construct asymmetric EAQECCs. Asymmetric EAQECCs arise after noting that in quantum error-correction we consider two different types of errors, phase-shift and qudit-flip errors, which are not equally likely to occur [15]. Asymmetric EAQECCs have two different error correction capabilities for each of the errors, which are expressed by two minimum distances, δ_z and δ_x, whose meaning is that the corresponding asymmetric EAQECC can correct up to $\lfloor(\delta_z-1)/2\rfloor$ phase-shift errors and $\lfloor(\delta_x-1)/2\rfloor$ qudit-flip errors.

Given a nonempty set $U \subset \mathbb{F}_q^n$, we denote by $\mathrm{wt}(U)$ the number $\min\{\mathrm{wt}(v) \mid v \in U\backslash\{0\}\}$. To construct asymmetric EAQECCs, we can use the following result from [11].

Theorem E.4.1. *Let $C_i \subset \mathbb{F}_q^n$ be linear codes of dimension k_i, for $i = 1, 2$. Then, there is an asymmetric EAQECC with parameters $[[n, \kappa, \delta_z/\delta_x; c]]_q$, where*

$$c = k_1 - \dim(C_1 \cap C_2^\perp),\ \kappa = n - (k_1 + k_2) + c,$$
$$\delta_z = \mathrm{wt}\left(C_1^\perp \setminus \left(C_1^\perp \cap C_2\right)\right) \text{ and } \delta_x = \mathrm{wt}\left(C_2^\perp \setminus \left(C_2^\perp \cap C_1\right)\right).$$

Symmetric quantum codes can also be obtained from the previous construction by considering the minimum distance $\delta = \min\{\delta_z, \delta_x\}$ instead of the two minimum distances δ_z and δ_x.

If $C_1 \subset C_2^\perp$, we have $c = 0$ and in that case we do not require entanglement assistance. The asymmetric EAQECC from the previous result is called *pure* if $\delta_z = \mathrm{wt}(C_1^\perp)$ and $\delta_x = \mathrm{wt}(C_2^\perp)$, and it is called *impure* otherwise. For the symmetric case, the code is called pure if $\delta = \min\{\mathrm{wt}(C_1^\perp), \mathrm{wt}(C_2^\perp)\}$, and impure otherwise.

Finding impure quantum codes is a difficult task in general. The following result supports this fact because it implies that the EAQECCs we obtain using projective Reed-Muller codes are always pure.

Lemma E.4.2. *Let $1 \le d_1, d_2 \le 2(q-1)$, with $d_1 \not\equiv d_2 \bmod q-1$. We have that*

$$\mathrm{wt}\left(\mathrm{PRM}_{d_1}(2) \setminus (\mathrm{PRM}_{d_1}(2) \cap \mathrm{PRM}_{d_2}(2))\right) = \mathrm{wt}(\mathrm{PRM}_{d_1}(2))$$

Proof. If $d_2 < d_1$, then $\mathrm{wt}(\mathrm{PRM}_{d_2}(2)) > \mathrm{wt}(\mathrm{PRM}_{d_1}(2))$. Therefore, there is a codeword of Hamming weight $\mathrm{wt}(\mathrm{PRM}_{d_1}(2))$ in $\mathrm{PRM}_{d_1}(2) \setminus \mathrm{PRM}_{d_2}(2)$.

On the other hand, if $d_2 > d_1$, we consider two cases. If $d_1 \leq q-1$, then the evaluation of the polynomial

$$x_2 \prod_{j=1}^{d_1-1} (\lambda_j x_2 - x_1),$$

where $\lambda_i \neq \lambda_j$ if $i \neq j$, $\lambda_j \in \mathbb{F}_q^*$, has Hamming weight $q(q-d_1+1) = \mathrm{wt}(\mathrm{PRM}_{d_1}(2))$. This is easy to check using the representatives $[\mathbb{F}_q^2 \times \{1\}] \cup [\mathbb{F}_q \times \{1\} \times \{0\}] \cup \{[1:0:0]\}$ for $\mathbb{P}^2$. This polynomial is not contained in $S_{d_1}/I(P^2) \cap S_{d_2}/I(P^2)$ because this vector space is generated by $A_1^{d_1} \cup \left(\bigcup_{a_2 \in Y} \{x_1^{d_1-a_2} x_2^{a_2}\}\right)$, which does not generate the monomial $x_2^{d_1}$ that is in the support of the previous polynomial. Thus, the evaluation of this polynomial is a codeword of Hamming weight $\mathrm{wt}(\mathrm{PRM}_{d_1}(2))$ in $\mathrm{PRM}_{d_1}(2) \setminus (\mathrm{PRM}_{d_1}(2) \cap \mathrm{PRM}_{d_2}(2))$.

If $d_1 \geq q$, we consider instead the polynomial

$$x_1(x_2^{q-1} - x_1^{q-1}) \prod_{j=1}^{\overline{d_1}-1} (\lambda_j x_1 - x_0), \tag{E.4.1}$$

where $\lambda_i \neq \lambda_j$ if $i \neq j$, $\lambda_j \in \mathbb{F}_q^*$. As before, it is easy to check that the evaluation of this polynomial has Hamming weight $q-\overline{d_1}+1 = \mathrm{wt}(\mathrm{PRM}_{d_1}(2))$. The monomial $x_1^{\overline{d_1}} x_2^{q-1}$ in the support of the previous polynomial is part of the basis from Lemma E.2.7. We have that $S_{d_2}/I(P^2) \cap S_{d_1}/I(P^2)$ is generated in this case by $A_1^{d_1} \cup \left(\bigcup_{a_2 \in Y} \{x_1^{d_1-a_2} x_2^{a_2}\}\right) \cup \{Q_{d_1,d_2}\}$. All of these monomials, and Q_{d_1,d_2}, are expressed in terms of the basis from Lemma E.2.7. Therefore, the only way to generate a polynomial with $x_1^{\overline{d_1}} x_2^{q-1}$ in its support is to have this monomial in the expression of some element of the basis of $S_{d_1}/I(P^2) \cap S_{d_2}/I(P^2)$ in terms of the basis from Lemma E.2.7. By checking the definitions, we see that this only happens if $\overline{d_2} = q-1$, because in that case this monomial appears in the expression of Q_{d_1,d_2}. However, Q_{d_1,d_2} has the monomial $x_2^{d_1}$ in its support, and the polynomial from (E.4.1) does not, and $x_2^{d_1}$ cannot be cancelled because no other monomial from the basis of $S_{d_1}/I(P^2) \cap S_{d_2}/I(P^2)$ has this monomial in its support. Hence, the evaluation of the polynomial from (E.4.1) gives a codeword of Hamming weight $\mathrm{wt}(\mathrm{PRM}_{d_1}(2))$ in $\mathrm{PRM}_{d_1}(2) \setminus (\mathrm{PRM}_{d_1}(2) \cap \mathrm{PRM}_{d_2}(2))$. □

Remark E.4.3. For $d_1 \equiv d_2 \bmod q-1$, if $d_2 < d_1$, then

$$\mathrm{wt}\left(\mathrm{PRM}_{d_1}(2) \setminus (\mathrm{PRM}_{d_1}(2) \cap \mathrm{PRM}_{d_2}(2))\right) = \mathrm{wt}(\mathrm{PRM}_{d_1}(2))$$

arguing as in the previous result. If $d_2 \geq d_1$, then

$$\mathrm{PRM}_{d_1}(2) \setminus (\mathrm{PRM}_{d_1}(2) \cap \mathrm{PRM}_{d_2}(2)) = \emptyset.$$

Now we show the parameters of the asymmetric EAQECCs arising from Theorem E.4.1 when C_1 and C_2 are projective Reed-Muller codes. Note that the parameters of $\mathrm{PRM}_d(2)$ and $\mathrm{RM}_d(2)$ are in Theorems E.2.1 and E.2.4, and for $\mathrm{PRM}_d^{\perp}(2)$ we can use Theorem E.2.2.

Theorem E.4.4. *Let $1 \leq d_1 \leq d_2 < 2(q-1)$, $d_1+d_2 \not\equiv 0 \bmod q-1$, $d_1 \neq q-1 \neq d_2$. Let $k_1 = \dim \mathrm{RM}_{d_1-1}(2)$ and $k_2 = \dim \mathrm{RM}_{d_2^{\perp}-1}(2)$, where $d_2^{\perp} = 2(q-1)-d_2$. Then we can*

construct an asymmetric EAQECC with parameters $[[n, \kappa, \delta_z/\delta_x; c]]_q$*, where* $n = q^2+q+1$, $\kappa = n - (\dim \mathrm{PRM}_{d_1}(2) + \dim \mathrm{PRM}_{d_2}(2)) + c$, $\delta_z = \mathrm{wt}(\mathrm{PRM}_{d_2}^{\perp}(2))$, $\delta_x = \mathrm{wt}(\mathrm{PRM}_{d_1}^{\perp}(2))$, *and the value of* c *is the following:*

1. *If* $d_1 + d_2 < 2(q-1)$*:*

$$c = \begin{cases} d_1 + 1 - \min\{d_1, q-1-d_2\} & \text{if } d_2 < q-1, \\ d_1 + 1 & \text{if } q \leq d_2. \end{cases}$$

2. *If* $d_1 + d_2 > 2(q-1)$*:*

$$c = \begin{cases} k_1 - k_2 + d_1 + 1 & \text{if } d_1 < q-1, \\ k_1 - k_2 + q + 1 - \min\{d_2^{\perp}, d_1 - (q-1)\} & \text{if } q \leq d_1. \end{cases}$$

Moreover, this code is pure.

Proof. We consider $C_1 = \mathrm{PRM}_{d_1}(2)$, $C_2 = \mathrm{PRM}_{d_2}(2)$, and apply Theorem E.4.1. For the parameter c, we use Corollary E.3.11 with d_1 and $d_2^{\perp} = 2(q-1) - d_2$, taking into account that $d_1 + d_2 \not\equiv 0 \bmod q-1$ implies that $d_1 \not\equiv 2(q-1) - d_2 \bmod q-1$, and Remark E.2.8. We also note that if $d_1 + d_2 < 2(q-1)$, then $d_1 < d_2^{\perp}$, and if $d_1 + d_2 > 2(q-1)$, then $d_2^{\perp} < d_1$.

A direct application of Theorem E.4.1 would give us a pure quantum code with $\delta_z = \mathrm{wt}(\mathrm{PRM}_{d_1}^{\perp}(2))$ and $\delta_x = \mathrm{wt}(\mathrm{PRM}_{d_2}^{\perp}(2))$ due to Lemma E.4.2. However, it is easy to see that if we exchange the roles of C_1 and C_2 in Theorem E.4.1, the resulting asymmetric EAQECC has the same parameters, except that δ_z and δ_x are exchanged, which gives the result. □

Let $d_1 \not\equiv 0 \bmod q-1$, $d_2 \not\equiv 0 \bmod q-1$. If $d_1 + d_2 = q-1$ or $d_1 + d_2 = 2(q-1)$, we can obtain an EAQECC as in Theorem E.4.4 with $c = 0$ because $\dim(\mathrm{PRM}_{d_1}(2) \cap \mathrm{PRM}_{d_2}^{\perp}(2)) = \dim \mathrm{PRM}_{d_1}(2)$ by Lemma E.3.1. If $d_1+d_2 = 3(q-1)$ or $d_1+d_2 = 4(q-1)$, we have $c = \dim \mathrm{PRM}_{d_1}(2) - \dim \mathrm{PRM}_{d_2}^{\perp}(2)$ instead, because $\dim(\mathrm{PRM}_{d_1}(2) \cap \mathrm{PRM}_{d_2}^{\perp}(2)) = \dim \mathrm{PRM}_{d_2}^{\perp}(2)$.

Example E.4.5. We consider $\mathbb{F}_q = \mathbb{F}_9$, and we use Theorem E.4.4 with $d_1 = 3$, $d_2 = 11$. The parameters for the corresponding affine and projective Reed-Muller codes are obtained from Theorem E.2.4 and Theorem E.2.1, respectively. For the parameter c, we have $d_1 + d_2 = 14 < 16 = 2(q-1)$, and $c = 3+1 = 4$ in this case because $q = 9 \leq 11 = d_2$. The asymmetric EAQECC that we obtain in this way has parameters $[[91, 15, 45/5; 4]]_9$. With affine Reed-Muller codes, it is possible to obtain an asymmetric EAQECC with parameters $[[81, 5, 45/5; 0]]_9$. If we define the rate as $\rho := \kappa/n$, and the net rate as $\overline{\rho} := (\kappa - c)/n$, we see that the projective code clearly has higher rate, but it also has higher net rate.

In [15] it is shown that the probability of phase-shift errors is between 10 and 100 times higher than the probability of qudit-flip errors, depending on the devices used for constructing qubits. Hence, it is desirable to construct EAQECCs with a higher correction capability for phase-shift errors, i.e., EAQECCs with $\delta_z \gg \delta_x$. The EAQECCs arising from Theorem E.4.4 automatically satisfy $\delta_z \geq \delta_x$. We show now how to construct codes with high asymmetry ratio δ_z/δ_x using projective Reed-Muller codes.

Example E.4.6. Assume that for a certain application we want to correct 1 qudit-flip error (and detect 2), for lengths lower than 200. Therefore, we want to obtain an asymmetric EAQECC with $\delta_x = 3$. If we assume that the probability of phase-shift errors is between 10 and 100 times higher than the probability of qudit-flip errors, we want to construct codes with δ_z between 30 and 300. If we consider the field $\mathbb{F}_q$, using Theorem E.4.4 it is easy to check that the asymmetric EAQECC with highest asymmetry ratio and nonzero dimension that we can obtain has parameters

$$[[q^2+q+1, 5, q(q-1)/3; 2]]_q,$$

which corresponds to $d_1 = 1$ and $d_2 = 2(q-1)-2$. By considering $q = 9, 11, 13$, we obtain the parameters $[[91, 5, 72/3; 2]]_9$, $[[133, 5, 110/3; 2]]_{11}$, $[[183, 5, 156/3; 2]]_{13}$, respectively. All of the previous codes satisfy the required conditions about the asymmetry ratio and length, and all of them surpass the quantum Gilbert Varshamov bound from [23].

With affine Reed-Muller codes we can obtain instead the parameters

$$[[q^2, 3, q(q-2)/3; 0]]_q.$$

Hence, with projective Reed-Muller codes we can achieve a higher asymmetry ratio, at the expense of getting a worse net rate with respect to the affine case. We can also obtain the same asymmetry ratio as with affine Reed-Muller codes, and increase the net rate, by using projective Reed-Muller codes as we saw in Example E.4.5.

It is not easy to compare the codes that we obtain with the literature because there are not many references about asymmetric EAQECCs. However, we can use the quantum Gilbert-Varshamov bound from [23] to argue that we are obtaining quantum codes with good parameters. In Table E.1 we show some of the codes that we obtain that surpass the quantum Gilbert-Varshamov bound from [23].

We turn our attention now to the symmetric case. Given a symmetric quantum code obtained using the construction from Theorem E.4.1 with parameters $[[n, \kappa, \delta; c]]_q$, we can define the rate and net rate as in Example E.4.5. Fixing the length and minimum distance, if an EAQECC has better net rate than other EAQECC, while keeping the other rate constant, we will say that the first code has better parameters than the second one. In this sense, for the symmetric codes arising from Theorem E.4.4, the following result shows that the best symmetric codes are obtained when $d_1 = d_2$.

Corollary E.4.7. *We fix $1 \leq d_1 < 2(q-1)$, and let $d_1 \leq d_2 < 2(q-1)$ with $d_1 \neq q-1 \neq d_2$ and $d_1 + d_2 \not\equiv 0 \bmod q-1$. Let $k_1 = \dim \mathrm{RM}_{d_1-1}(2)$ and $k_2 = \dim \mathrm{RM}_{d_2^\perp-1}(2)$, where $d_2^\perp = 2(q-1)-d_2$. Then the best choice for d_2 in Theorem E.4.4 for symmetric EAQECCs is $d_2 = d_1$, which gives an EAQECC with parameters $[[n, \kappa, \delta; c]]$, where $n = q^2+q+1$, $\kappa = n - 2(\dim \mathrm{PRM}_{d_1}(2)) + c$, $\delta = \mathrm{wt}(\mathrm{PRM}_{d_1}^\perp(2))$, and*

$$c = \begin{cases} d_1 + 1 - \min\{d_1, q-1-d_1\} & \text{if } d_1 < (q-1), \\ k_1 - k_2 + q + 1 - \min\{d_1^\perp, d_1 - (q-1)\} & \text{if } d_1 > (q-1). \end{cases}$$

Proof. For $d_2 \geq d_1$, we have that $\min\{\mathrm{wt}(\mathrm{PRM}_{d_1}^\perp(2)), \mathrm{wt}(\mathrm{PRM}_{d_2}^\perp(2))\} = \mathrm{wt}(\mathrm{PRM}_{d_1}^\perp(2))$ from Theorem E.2.2. Therefore, all the symmetric EAQECCs obtained from Theorem E.4.4 in this setting have the same parameter δ. For $d_1 = d_2$, we obtain from Theorem

Table E.1: Codes arising from Theorem E.4.4 surpassing the quantum Gilbert-Varshamov bound from [23].

q	d_1	d_2	n	κ	δ_x	δ_z	c	q	d_1	d_2	n	κ	δ_x	δ_z	c
4	1	1	21	16	3	3	1	9	1	14	91	5	3	72	2
4	1	4	21	5	3	12	2	9	2	2	91	80	4	4	1
4	2	2	21	11	4	4	2	9	2	3	91	76	4	5	1
4	2	5	21	2	4	16	5	9	2	11	91	18	4	45	3
4	4	4	21	2	12	12	11	9	2	12	91	12	4	54	3
4	5	5	21	1	16	16	16	9	2	13	91	7	4	63	3
5	1	1	31	26	3	3	1	9	2	15	91	2	4	81	5
5	1	2	31	23	3	4	1	9	3	3	91	72	5	5	1
5	1	5	31	9	3	15	2	9	3	12	91	9	5	54	4
5	1	6	31	5	3	20	2	9	3	14	91	3	5	72	7
5	2	3	31	17	4	5	2	9	3	15	91	2	5	81	9
5	2	5	31	7	4	15	3	9	4	13	91	4	6	63	9
5	2	7	31	2	4	25	5	9	4	14	91	3	6	72	12
5	3	6	31	3	5	20	7	9	4	15	91	2	6	81	14
5	3	7	31	2	5	25	9	9	11	12	91	2	45	54	57
5	5	5	31	3	15	15	14	9	11	14	91	1	45	72	65
5	5	6	31	2	15	20	17	9	11	15	91	1	45	81	68
5	6	7	31	1	20	25	23	9	12	13	91	1	54	63	67
5	7	7	31	1	25	25	26	9	12	14	91	1	54	72	71
9	1	1	91	86	3	3	1	9	12	15	91	1	54	81	74
9	1	2	91	83	3	4	1	9	13	13	91	1	63	63	72
9	1	3	91	79	3	5	1	9	13	14	91	1	63	72	76
9	1	4	91	74	3	6	1	9	13	15	91	1	63	81	79
9	1	11	91	20	3	45	2	9	14	14	91	1	72	72	80
9	1	12	91	14	3	54	2	9	14	15	91	1	72	81	83
9	1	13	91	9	3	63	2	9	15	15	91	1	81	81	86

E.4.4 an EAQECC with the stated parameters. For $d_2 > d_1$ such that $d_2 \neq q-1$ and $d_2 < 2(q-1)$, we will see that we obtain a worse code. We have that $\dim \mathrm{PRM}_{d_2}(2) > \dim \mathrm{PRM}_{d_1}(2)$ if $d_2 > d_1$, which decreases the dimension of the corresponding EAQECC with respect to the one obtained with $d_1 = d_2$. From Theorem E.4.4, we also see that c is either going to increase or be the same (if $d_1 + d_2 \not\equiv 0 \bmod q-1$). Hence, in the sense stated before, the corresponding EAQECC with $d_2 > d_1$ has worse parameters than the one obtained with $d_1 = d_2$ because it has less dimension while not decreasing the parameter c, which gives a worse rate and net rate. □

E.4.2 Hermitian EAQECCs

In this subsection we construct EAQECCs using the following Hermitian construction from [10].

Theorem E.4.8 (Hermitian construction)**.** *Let $C \subset \mathbb{F}_{q^2}^n$ be a linear code of dimension k and $C^{\perp_h}$ its Hermitian dual. Then, there is an EAQECC with parameters $[[n, \kappa, \delta; c]]_q$,*

where

$$c = k - \dim(C \cap C^{\perp_h}),\ \kappa = n - 2k + c, \quad \textit{and} \ \ \delta = \mathrm{wt}(C^{\perp_h} \setminus (C \cap C^{\perp_h})).$$

We see that we can use the knowledge of the Hermitian hull from Theorem E.3.23 and Corollary E.3.28 to compute the parameter c of the EAQECCs obtained from the previous result using projective Reed-Muller codes.

Theorem E.4.9. *Let $1 \leq d < q^2-1$. Then we can construct an EAQECC with parameters $[[n, \kappa, \delta; c]]_q$, where $n = q^4+q^2+1$, $\kappa = n-2(\dim \mathrm{PRM}_d(q^2,2))+c$, $\delta \geq \mathrm{wt}(\mathrm{PRM}_d^{\perp}(q^2,2))$, and the value of c is given by the following:*

If $d \leq 2(q-1)$:

$$c = \begin{cases} 0 & \textit{if } d \equiv 0 \bmod q-1, \\ 1 & \textit{if } 1 \leq d < q-1, \\ 2 & \textit{if } q-1 < d < 2(q-1). \end{cases}$$

If $d > 2(q-1)$ and $d \equiv 0 \bmod q-1$, then

$$c = \dim \mathrm{RM}_{d-1}(q^2,2) - |U|,$$

and if $d > 2(q-1)$, $d \not\equiv 0 \bmod q-1$, then we have the upper bound

$$c \leq \dim \mathrm{RM}_{d-1}(q^2,2) - |U| + d - |V| - |W| + 1.$$

Proof. We consider $C = \mathrm{PRM}_d(q^2,2)$ and we use the Hermitian Construction from Theorem E.4.8. We only need to prove the statements about the parameter

$$c = \dim \mathrm{PRM}_d(q^2,2) - \dim(\mathrm{PRM}_d(q^2,2) \cap \mathrm{PRM}_d^{\perp_h}(q^2,2)),$$

for which we will use Corollary E.3.28.

First, we recall that $\dim \mathrm{PRM}_d(q^2,2) = |A_1^d| + |A_2^d| + |A_3^d| = \dim \mathrm{RM}_{d-1}(q^2,2) + d + 1$ (see Remark E.2.8). If $d \equiv 0 \bmod q-1$, by Theorem E.3.23 we have that $c = |A_1^d| - |U| = \dim \mathrm{RM}_{d-1}(q^2,2) - |U|$. For the case with $1 \leq d \leq 2(q-1)$, we also have to consider Lemma E.3.17.

Now we assume $d \not\equiv 0 \bmod q-1$. If $d \leq 2(q-1)$, by Corollary E.3.28 we would have

$$c = \dim \mathrm{PRM}_d(q^2,2) - |U| - |V| = 1 + \beta_1^2.$$

We have $\beta_1 = 0$ for $1 \leq d < q-1$ and $\beta_1 = 1$ for $q-1 < d \leq 2(q-1)$, which completes this case.

Finally, if $d > 2(q-1)$, we use Corollary E.3.28 to finish the proof. □

Remark E.4.10. For $2(q-1) < d \leq q^2-1$, $d \not\equiv 0 \bmod q-1$, we can write

$$\dim \mathrm{RM}_{d-1}(q^2,2) - |U| + d - |V| - |W| + 1 = \dim \mathrm{PRM}_d(q^2,2) - |U| - |V| - |W|.$$

We also note that $|V| + |W| \geq |V| = |T|$, but it is not necessarily equal (this would give a worse upper bound than the one given in the result). The bound given in Theorem E.4.9 for c is sharp in all cases we have checked, but if we use $|T|$ instead of $|V|+|W|$ the bound is not always sharp. We also note that we have formulas for $|V| = |T|$ and $|U|$ in Lemma E.3.25 and Lemma E.5.1 (in the Appendix), respectively.

Example E.4.11. Let $q = 3$. For $d = 1, 2, 3$, using Theorem E.4.9 we obtain the parameters $[[91, 85, 3; 1]]_3$, $[[91, 79, 4; 0]]_3$ and $[[91, 71, 5; 2]]_3$, respectively. All of these codes surpass the quantum Gilbert Varshamov bound from [23]. Moreover, the code with $c = 0$ surpasses the quantum Gilbert-Varshamov bound from [9], which seems to be more difficult to surpass than the one from [23] for the case $c = 0$.

As we stated in Remark E.3.19, we are also able to compute the dimension of the Hermitian hull for affine Reed-Muller codes in the case $m = 2$, therefore obtaining the following result.

Theorem E.4.12. *Let $0 \leq d < q^2 - 1$. Then we can construct an EAQECC with parameters $[[n, \kappa, \delta; c]]_q$, where $n = q^4$, $\kappa = n - 2(\dim \mathrm{RM}_d(q^2, 2)) + c$, $\delta \geq \mathrm{wt}(\mathrm{RM}_d^{\perp}(q^2, 2))$, and the value of c is*

$$c = \begin{cases} 0 & \text{if } d < 2(q-1), \\ \dim \mathrm{RM}_d(q^2, 2) - |U_{d,d}| & \text{if } d \geq 2(q-1), \end{cases}$$

where $|U_{d,d}|$ is given by the expression in Remark E.5.2.

Proof. This is a consequence of Proposition E.3.15 and Proposition E.3.13. □

Remark E.4.13. By Remark E.5.2, $|U_{d,d}|$ is given by the same expression as $|U|$ in Lemma E.5.1, but considering $d = \beta_0 + \beta_1 q$ instead.

E.5 Appendix

In this appendix we provide an explicit formula for $|U|$, which appears in the computation of the dimension of the Hermitian hull of projective Reed-Muller codes from Corollary E.3.23. This formula can also be used for the dimension of the Hermitian hull of affine Reed-Muller codes (see Remark E.5.2).

Lemma E.5.1. *Let $1 \leq d < q^2 - 1$ with q-adic expansion $d - 1 = \beta_0 + \beta_1 q$ and let $d^{\perp} = 2(q^2 - 1) - d$. We also consider the q-adic expansion $d^{\perp} = \lambda_0 + \lambda_1 q + q^2$. Then, we have*

$$|U| = \dim \mathrm{RM}_{d-1}(q^2, 2) - \sum_{i=1}^{4} B_i, \tag{E.5.1}$$

where

$$B_1 = \binom{q - \lambda_1 - 1}{q - \lambda_1 - 3} \binom{\beta_1}{\beta_1 - 2}, B_2 = \max\left\{ \beta_1 \left[\binom{q - \lambda_1 - 1}{q - \lambda_1 - 3} - \binom{q - \beta_0 - 1}{q - \beta_0 - 3} \right], 0 \right\},$$

$$B_3 = \max\left\{ (q - 1 - \lambda_1) \left[\binom{\beta_1}{\beta_1 - 2} - \binom{\lambda_0 + 1}{\lambda_0 - 1} \right], 0 \right\},$$

$$B_4 = \beta_1 (q - 1 - \lambda_1) \binom{\beta_0 - \lambda_1}{\beta_0 - \lambda_1} \binom{\beta_1 - \lambda_0 - 1}{\beta_1 - \lambda_0 - 1}.$$

Proof. The number of monomials $x_1^{a_1} x_2^{a_2}$ such that $0 \leq a_1, a_2 \leq q^2 - 1$ and $a_1 + a_2 \leq d - 1$ is precisely $\dim \mathrm{RM}_{d-1}(2)$. Now we compute the number of monomials that do not satisfy

the condition $\overline{qa_1} + \overline{qa_2} \leq d^\perp - 1$, i.e., the monomials such that $\overline{qa_1} + \overline{qa_2} \geq d^\perp$,and by subtracting this number from $\dim \mathrm{RM}_d(2)$ we obtain the cardinal of the set U.

Given $x_1^{a_1}x_2^{a_2}$ with $a_1 + a_2 \leq d - 1$ and $1 \leq a_1, a_2 \leq q^2 - 1$, we consider the q-adic expansions $a_1 = \alpha_0 + \alpha_1 q$ and $a_2 = \gamma_0 + \gamma_1 q$. Then we have $a_1 + a_2 = (\alpha_0 + \gamma_0) + (\alpha_1 + \gamma_1)q$. Moreover, it is easy to check that $\overline{qa_1} + \overline{qa_2} = (\alpha_1 + \gamma_1) + (\alpha_0 + \gamma_0)q$. However, these last expressions for $a_1 + a_2$ and $\overline{qa_1} + \overline{qa_2}$ are not their q-adic expansions in general. We separate cases according to the different possible q-adic expansions for these integers, and in each case we consider the monomials $x_1^{a_1}x_2^{a_2}$ such that $a_1 + a_2 \leq d - 1$ and $\overline{qa_1} + \overline{qa_2} \geq d^\perp$.

(a) If $\alpha_0 + \gamma_0 \leq q - 1$ and $\alpha_1 + \gamma_1 \leq q - 1$: we have the q-adic expansions $a_1 + a_2 = (\alpha_0 + \gamma_0) + (\alpha_1 + \gamma_1)q$ and $\overline{qa_1} + \overline{qa_2} = (\alpha_1 + \gamma_1) + (\alpha_0 + \gamma_0)q$. The condition $\overline{qa_1} + \overline{qa_2} \geq d^\perp$ cannot be satisfied in this case because $\overline{qa_1} + \overline{qa_2} < q^2$, while $d^\perp \geq q^2$ (because $d < q^2 - 1$). Therefore, no monomial of this type satisfies $\overline{qa_1} + \overline{qa_2} \geq d^\perp$.

(b) If $\alpha_0 + \gamma_0 \leq q - 1$ and $\alpha_1 + \gamma_1 \geq q$: we have the q-adic expansion $a_1 + a_2 = (\alpha_0 + \gamma_0) + (\alpha_1 + \gamma_1 - q)q + q^2$, which implies $a_1 + a_2 \geq q^2 > d$, a contradiction with the fact that $a_1 + a_2 \leq d - 1$.

(c) If $\alpha_0 + \gamma_0 \geq q$ and $\alpha_1 + \gamma_1 + 1 \geq q$: we have the q-adic expansion $a_1 + a_2 = (\alpha_0 + \gamma_0 - q) + (\alpha_1 + \gamma_1 + 1 - q)q + q^2$, which implies that $a_1 + a_2 \geq q^2 > d$, a contradiction.

(d) If $\alpha_0 + \gamma_0 \geq q$ and $\alpha_1 + \gamma_1 + 1 \leq q - 1$: we have the q-adic expansions $a_1 + a_2 = (\alpha_0 + \gamma_0 - q) + (\alpha_1 + \gamma_1 + 1)q$ and $\overline{qa_1} + \overline{qa_2} = (\alpha_1 + \gamma_1) + (\alpha_0 + \gamma_0 - q)q + q^2$. In this case, we can have monomials satisfying the required conditions.

Now we count the monomials that we consider in the case (d). The condition $a_1 + a_2 \leq d - 1$ implies that $\alpha_1 + \gamma_1 + 1 < \beta_1$ or $\alpha_1 + \gamma_1 + 1 = \beta_1$ and $\alpha_0 + \gamma_0 - q \leq \beta_0$. The condition $\overline{qa_1} + \overline{qa_2} \geq d^\perp$ implies that $\alpha_0 + \gamma_0 - q > \lambda_1$ or $\alpha_0 + \gamma_0 - q = \lambda_1$ and $\alpha_1 + \gamma_1 \geq \lambda_0$. Hence, we have four possibilities, and we are going to compute the number of monomials satisfying each of the four possible combinations of conditions.

1. If $\alpha_1 + \gamma_1 + 1 < \beta_1$, $\alpha_0 + \gamma_0 - q > \lambda_1$: for each value $\alpha_1 \in \{0, \ldots, q - 1\}$, γ_1 can take any value from $\{0, \ldots, \beta_1 - 2 - \alpha_1\}$. It is not hard to check that this gives $\binom{\beta_1}{\beta_1 - 2}$ possible choices for the pair (α_1, γ_1). Similarly, for each value of $\alpha_0 \in \{1, \ldots, q - 1\}$ (recall that we need to have $\alpha_0 + \gamma_0 \geq q$, and $\alpha_0, \gamma_0 \leq q - 1$), we have that γ_0 can take any value in $\{\lambda_1 + q - \alpha_0 + 1, \ldots, q - 1\}$. Similarly to the previous case, this gives $\binom{q - \lambda_1 - 1}{q - \lambda_1 - 3}$ possible choices for the pair (α_0, γ_0). Thus, we obtain

$$B_1 = \binom{q - \lambda_1 - 1}{q - \lambda_1 - 3}\binom{\beta_1}{\beta_1 - 2}$$

monomials in this case.

2. If $\alpha_1 + \gamma_1 + 1 = \beta_1$, $\alpha_0 + \gamma_0 - q \leq \beta_0$, $\alpha_0 + \gamma_0 - q > \lambda_1$: we have β_1 possible choices for (α_1, γ_1), and for α_0, γ_0 we have the condition $\lambda_1 < \alpha_0 + \gamma_0 - q \leq \beta_0$. Note that this can only happen if $\lambda_1 < \beta_0$. Assuming $\lambda_1 < \beta_0$, we can compute the number of (α_0, γ_0) such that $\lambda_1 < \alpha_0 + \gamma_0 - q$, and subtract the number of (α_0, γ_0) such that

$\beta_0 < \alpha_0 + \gamma_0 - q$. These numbers can be computed as in the previous case, and multiplying by β_1 (to take into account the possible (α_1, γ_1)) we obtain

$$\beta_1 \left[\binom{q-\lambda_1-1}{q-\lambda_1-3} - \binom{q-\beta_0-1}{q-\beta_0-3} \right]$$

monomials for the case $\lambda_1 < \beta_0$, and 0 otherwise, which is precisely the number B_2 in the statement.

3. If $\alpha_1+\gamma_1+1 < \beta_1$, $\alpha_0+\gamma_0-q = \lambda_1$, $\alpha_1+\gamma_1 \geq \lambda_0$: we can argue in the same way as the last case, taking into account that in this case we only obtain a nonzero amount of monomials if $\lambda_0 < \beta_1 - 1$. Thus, we obtain

$$B_3 = \max\left\{ (q-1-\lambda_1) \left[\binom{\beta_1}{\beta_1-2} - \binom{\lambda_0+1}{\lambda_0-1} \right], 0 \right\}$$

monomials.

4. If $\alpha_1+\gamma_1+1 = \beta_1$, $\alpha_0+\gamma_0-q \leq \beta_0$, $\alpha_0+\gamma_0-q = \lambda_1$, $\alpha_1+\gamma_1 \geq \lambda_0$: in this case we obtain $\beta_1(q-1-\lambda_1)$ monomials, but only if $\beta_1 - 1 \geq \lambda_0$ and $\lambda_1 \leq \beta_0$. Therefore, there are

$$B_4 = \beta_1(q-1-\lambda_1)\binom{\beta_0-\lambda_1}{\beta_0-\lambda_1}\binom{\beta_1-\lambda_0-1}{\beta_1-\lambda_0-1}$$

monomials of this type. Note that the product of the combinatorial numbers that appear in B_4 is 1 when $\beta_0 - \lambda_1 \geq 0$ and $\beta_1 - \lambda_0 - 1 \geq 0$, and 0 otherwise.

Hence, the size of the set U is given by

$$\dim \mathrm{RM}_{d-1}(q^2, 2) - \sum_{i=1}^{4} B_i.$$

□

Remark E.5.2. For the affine case, if $d = \beta_0 + \beta_1 q$ is the q-adic expansion of d instead of $d-1$, the proof of Lemma E.5.1 shows that

$$|U_{d,d}| = \dim \mathrm{RM}_d(q^2, 2) - \sum_{i=1}^{4} B_i.$$

This gives the dimension of the Hermitian hull for affine Reed-Muller codes in 2 variables.

E.6 Acknowledgements

We would like to thank Nathan Kaplan and Jon-Lark Kim for their careful reading of this article and for pointing out a typo in a previous version of this manuscript.

Bibliography

[1] S. E. Anderson, E. Camps-Moreno, H. H. López, G. L. Matthews, D. Ruano, and I. Soprunov. Relative hulls and quantum codes. *IEEE Trans. Inform. Theory*, 70(5):3190–3201, 2024.

[2] S. Ball. Some constructions of quantum MDS codes. *Des. Codes Cryptogr.*, 89(5):811–821, 2021.

[3] P. Beelen, M. Datta, and S. R. Ghorpade. Vanishing ideals of projective spaces over finite fields and a projective footprint bound. *Acta Math. Sin. (Engl. Ser.)*, 35(1):47–63, 2019.

[4] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[5] T. Brun, I. Devetak, and M.-H. Hsieh. Correcting quantum errors with entanglement. *Science*, 314(5798):436–439, 2006.

[6] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane. Quantum error correction via codes over GF(4). *IEEE Trans. Inform. Theory*, 44(4):1369–1387, 1998.

[7] D. A. Cox, J. Little, and D. O'Shea. *Ideals, varieties, and algorithms*. Undergraduate Texts in Mathematics. Springer, Cham, fourth edition, 2015. An introduction to computational algebraic geometry and commutative algebra.

[8] P. Delsarte, J.-M. Goethals, and F. J. MacWilliams. On generalized Reed-Muller codes and their relatives. *Information and Control*, 16:403–442, 1970.

[9] K. Feng and Z. Ma. A finite Gilbert-Varshamov bound for pure stabilizer quantum codes. *IEEE Trans. Inform. Theory*, 50(12):3323–3325, 2004.

[10] C. Galindo, F. Hernando, R. Matsumoto, and D. Ruano. Entanglement-assisted quantum error-correcting codes over arbitrary finite fields. *Quantum Inf. Process.*, 18(4):Paper No. 116, 18, 2019.

[11] C. Galindo, F. Hernando, R. Matsumoto, and D. Ruano. Asymmetric entanglement-assisted quantum error-correcting codes and bch codes. *IEEE Access*, 8:18571–18579, 2020.

[12] C. Galindo, F. Hernando, and D. Ruano. Stabilizer quantum codes from J-affine variety codes and a new Steane-like enlargement. *Quantum Inf. Process.*, 14(9):3211–3231, 2015.

[13] P. Gimenez, D. Ruano, and R. San-José. Entanglement-assisted quantum error-correcting codes from subfield subcodes of projective Reed-Solomon codes. *Comput. Appl. Math.*, 42(8):Paper No. 363, 31, 2023.

[14] P. Gimenez, D. Ruano, and R. San-José. Subfield subcodes of projective Reed-Muller codes. *Finite Fields Appl.*, 94:Paper No. 102353, 46, 2024.

[15] L. Ioffe and M. Mézard. Asymmetric quantum error-correcting codes. *Phys. Rev. A*, 75:032345, Mar 2007.

[16] D. Jaramillo, M. Vaz Pinto, and R. H. Villarreal. Evaluation codes and their basic parameters. *Des. Codes Cryptogr.*, 89(2):269–300, 2021.

[17] N. Kaplan and J.-L. Kim. Hulls of Projective Reed-Muller Codes. *ArXiv 2406.04757*, 2024.

[18] T. Kasami, S. Lin, and W. W. Peterson. New generalizations of the Reed-Muller codes. I. Primitive codes. *IEEE Trans. Inform. Theory*, IT-14:189–199, 1968.

[19] A. Ketkar, A. Klappenecker, S. Kumar, and P. K. Sarvepalli. Nonbinary stabilizer codes over finite fields. *IEEE Trans. Inform. Theory*, 52(11):4892–4914, 2006.

[20] G. Lachaud. The parameters of projective Reed-Muller codes. *Discrete Math.*, 81(2):217–221, 1990.

[21] H. H. López, I. Soprunov, and R. H. Villarreal. The dual of an evaluation code. *Des. Codes Cryptogr.*, 89(7):1367–1403, 2021.

[22] J. Martínez-Bernal, Y. Pitones, and R. H. Villarreal. Minimum distance functions of graded ideals and Reed-Muller-type codes. *J. Pure Appl. Algebra*, 221(2):251–275, 2017.

[23] R. Matsumoto. Improved Gilbert–Varshamov bound for Entanglement-Assisted Asymmetric Quantum Error Correction by Symplectic Orthogonality. *IEEE Trans. Quantum Eng.*, 1:1–4, 2020.

[24] P. Sarvepalli and A. Klappenecker. Nonbinary quantum reed-muller codes. In *Proceedings. International Symposium on Information Theory, 2005. ISIT 2005.*, pages 1023–1027, 2005.

[25] P. K. Sarvepalli, S. A. Aly, and A. Klappenecker. Nonbinary stabilizer codes. In *Mathematics of quantum computation and quantum technology*, Chapman & Hall/CRC Appl. Math. Nonlinear Sci. Ser., pages 287–308. Chapman & Hall/CRC, Boca Raton, FL, 2008.

[26] P. Shor. Fault-tolerant quantum computation. In *Proceedings of 37th Conference on Foundations of Computer Science*, pages 56–65, 1996.

[27] A. B. Sørensen. Projective Reed-Muller codes. *IEEE Trans. Inform. Theory*, 37(6):1567–1576, 1991.

[28] A. M. Steane. Simple quantum error-correcting codes. *Phys. Rev. A (3)*, 54(6):4741–4751, 1996.

[29] A. M. Steane. Quantum Reed-Muller codes. *IEEE Trans. Inform. Theory*, 45(5):1701–1703, 1999.

Paper F

Quantum error-correcting codes from projective Reed-Muller codes and their hull variation problem

Diego Ruano, Rodrigo San-José

Abstract

Long quantum codes using projective Reed-Muller codes are constructed. Projective Reed-Muller codes are evaluation codes obtained by evaluating homogeneous polynomials at the projective space. We obtain asymmetric and symmetric quantum codes by using the CSS construction and the Hermitian construction, respectively. We provide entanglement-assisted quantum error-correcting codes from projective Reed-Muller codes with flexible amounts of entanglement by considering equivalent codes. Moreover, we also construct quantum codes from subfield subcodes of projective Reed-Muller codes.

Keywords: Projective Reed-Muller codes, quantum codes, subfield subcodes, Hermitian product, hull.

MSC: 81P70, 94B05, 13P25.

DOI: 10.48550/arXiv.2312.15308

Reference: D Ruano, R. San-José. Quantum error-correcting codes from projective Reed-Muller codes and their hull variation problem. ArXiv 2312.15308 (2024).

Affiliation: Diego Ruano, Rodrigo San-José: IMUVA-Mathematics Research Institute, Universidad de Valladolid.

F.1 Introduction

Stabilizer quantum error-correcting codes (QECCs) can be defined from classical linear codes. They can be defined from a pair of self-orthogonal classical linear codes with respect to the Euclidean inner product, CSS construction, and from a self-orthogonal classical linear code with respect to the Hermitian inner product, Hermitian construction [6,18,29]. Moreover, by sharing entanglement between encoder and decoder, it is possible to increase the communication capacity and remove the self-orthogonality condition, giving rise to entanglement-assisted quantum error-correcting codes (EAQECCs) [5]. For the CSS-like construction, the minimum number of maximally entangled quantum states required is equal to $c := \dim C_1 - \dim C_1 \cap C_2^{\perp}$. Therefore, the dimension of the *relative hull of* C_1 *with respect to* C_2, which is defined in [1] as $\mathrm{Hull}_{C_2}(C_1) := C_1 \cap C_2^{\perp}$, determines the parameter c. For the Hermitian construction, we only use one code C, and the parameter c is given by $\dim C - \dim C \cap C^{\perp_h}$, where $C^{\perp_h}$ is the Hermitian dual of C. The *Hermitian hull* of C is thus defined as $\mathrm{Hull}_H(C) := C \cap C^{\perp_h}$. Moreover, both QECCs and EAQECCs can be considered in an asymmetric fashion taking advantage of the asymmetry in quantum errors since phase-shift errors are more probable than qudit-flip errors [11, 16, 27].

In this paper, we construct QECCs and EAQECCs from projective Reed-Muller codes, which is a family of evaluation codes obtained by evaluating homogeneous polynomials of a given degree at the projective space [19, 28]. In [19], it is shown that these codes can outperform affine Reed-Muller codes in some instances. In general, one needs to require entanglement assistance when working with evaluation codes over the projective space, in particular, because the resulting families of codes are not necessarily nested. EAQECCs from projective Reed-Muller codes have been studied in [13, 14, 24], and in [26] for the few cases in which one has the nested condition. In Section F.3, we deal with asymmetric quantum codes coming from the CSS construction, and, in Section F.4, we deal with (symmetric) quantum codes coming from the Hermitian construction.

More concretely, we provide EAQECCs with a flexible amount of entanglement and unassisted EAQECCs, that is, the parameter c is equal to zero, which simply corresponds to the case of QECCs. We achieve this by considering equivalent linear codes whose (relative) hull has different dimension, i.e., we consider the so-called hull variation problem for projective Reed-Muller codes (following the terminology from [7]). We remark that it is always possible to increase the parameter c one by one [1, 20], for $q > 2$, however, one can only decrease the parameter c under certain conditions [1, 7], for $q > 2$. Note that, by considering equivalent codes that give rise to a different parameter c, the rate of the quantum code varies but the net rate is preserved (see Remark F.3.2 for details). Having a rich family of codes with the same net rate but with a different minimum number of entangled quantum states provides flexibility for practical applications. Moreover, the unassisted case is especially interesting, $c = 0$, since it has a simpler implementation. This corresponds to the case where the dimension of the relative hull is equal to $\dim C_1$ or the dimension of the Hermitian hull is equal to $\dim C$.

For both constructions, in Sections F.3 and F.4, we find conditions to obtain unassisted QECC by using projective Reed-Muller codes, obtaining asymmetric and symmetric quantum codes with good parameters, they surpass the Gilbert-Varhsamov bound [9,22]. Moreover, we show that the quantum codes obtained outperform the ones obtained from affine Reed-Muller codes. On top of this, we consider quantum codes from the subfield subcodes

of projective Reed-Muller codes. That is, given $C \subset \mathbb{F}_{q^s}^n$, we consider $C_q := C \cap \mathbb{F}_q^n$, its *subfield subcode* with respect to the extension $\mathbb{F}_{q^s}/\mathbb{F}_q$. We remark that this approach is not usually fruitful for this family of codes since one does not have conditions for having nested codes. Nevertheless, we are able to find certain technical conditions that allow us to consider subfield subcodes and construct long quantum codes over small finite fields.

F.2 Preliminaries

Let $\mathbb{F}_q$ be the finite field with q elements. We denote by $\mathbb{P}^m$ the projective space over $\mathbb{F}_q$. We choose for $\mathbb{P}^m$ the standard representatives, i.e., the representatives whose leftmost coordinate is equal to 1. If we regard the standard representatives as points in the affine space $\mathbb{A}^{m+1}$, we obtain the set $P^m := \{Q_1, \ldots, Q_n\} \subset \mathbb{A}^{m+1}$, where $n = |P^m| = \frac{q^{m+1}-1}{q-1}$.

Let $S = \mathbb{F}_q[x_0, \ldots, x_m]$. Given d a positive integer, we denote $S_d \subset S$ the set of homogeneous polynomials of degree d. We define the evaluation map

$$\mathrm{ev} : S_d \to \mathbb{F}_q^n, \;\; f \mapsto (f(Q_1), \ldots, f(Q_n)) \,.$$

The image of ev is the *projective Reed-Muller code of degree* d, denoted by $\mathrm{PRM}_d(q, m)$, or $\mathrm{PRM}_d(m)$ if there is no confusion about the field. For the minimum distance of a code $C \subset \mathbb{F}_q^n$, we use the notation $\mathrm{wt}(C)$. We have the following results about the parameters of projective Reed-Muller codes and their duality from [28] (also see [12]).

Theorem F.2.1. *The projective Reed-Muller code* $\mathrm{PRM}_d(q, m)$, $1 \leq d \leq m(q-1)$, *is an* $[n, k]$*-code with*

$$n = \frac{q^{m+1}-1}{q-1},$$
$$k = \sum_{t \equiv d \bmod q-1, 0<t\leq d} \left(\sum_{j=0}^{m+1} (-1)^j \binom{m+1}{j} \binom{t-jq+m}{t-jq} \right).$$

For the minimum distance, we have

$$\mathrm{wt}(\mathrm{PRM}_d(q, m)) = (q-\ell)q^{m-r-1}, \;\; \textit{where} \;\; d-1 = r(q-1)+\ell, \; 0 \leq \ell < q-1.$$

Theorem F.2.2. *Let* $1 \leq d \leq m(q-1)$ *and let* $d^\perp = m(q-1) - d$. *Then*

$$\mathrm{PRM}_d^\perp(q, m) = \mathrm{PRM}_{d^\perp}(q, m) \qquad \textit{if } d \not\equiv 0 \bmod (q-1),$$
$$\mathrm{PRM}_d^\perp(q, m) = \mathrm{PRM}_{d^\perp}(q, m) + \langle (1, \ldots, 1) \rangle \qquad \textit{if } d \equiv 0 \bmod (q-1).$$

With respect to affine Reed-Muller codes, we will denote them by $\mathrm{RM}_d(q, m)$, or by $\mathrm{RM}_d(m)$ if there is no confusion about the field. We recall now the analogous results for affine Reed-Muller codes [8, 17].

Theorem F.2.3. *The Reed-Muller code* $\mathrm{RM}_d(q, m)$, $1 \leq d \leq m(q-1)$, *is an* $[n, k]$*-code with*

$$n = q^m,$$
$$k = \sum_{t=0}^{d} \sum_{j=0}^{m} (-1)^j \binom{m}{j} \binom{t-jq+m-1}{t-jq}.$$

For the minimum distance, we have

$$\mathrm{wt}(\mathrm{RM}_d(q,m)) = (q-\ell)q^{m-r-1}, \text{ where } d = r(q-1)+\ell,\ 0 \le \ell < q-1.$$

Theorem F.2.4. *Let* $1 \le d \le m(q-1)$. *Then*

$$\mathrm{RM}_d^{\perp}(q,m) = \mathrm{RM}_{m(q-1)-d-1}(q,m).$$

For comparisons between the projective case and the affine case, it is important to note that $\mathrm{wt}(\mathrm{PRM}_d(q,m)) = \mathrm{wt}(\mathrm{RM}_{d-1}(q,m))$.

Regarding quantum codes, we will consider the CSS construction and the Hermitian construction. For the CSS construction, we are considering asymmetric QECCs. In quantum error-correction we may consider two different types of errors, phase-shift errors and qudit-flip errors. As the likelihood of occurrence of each type of error is different [16], it is desirable to have different error correction capabilities for each type of error, which is what asymmetric QECCs accomplish. Asymmetric QECCs have two minimum distances, δ_z and δ_x, meaning that they can correct up to $\lfloor(\delta_z-1)/2\rfloor$ phase-shift errors and $\lfloor(\delta_x-1)/2\rfloor$ qudit-flip errors. We denote the parameters of an asymmetric EAQECC by $[[n,\kappa,\delta_z/\delta_x;c]]_q$, where n is the length, κ is the dimension, and c is the minimum number of maximally entangled quantum qudit pairs required. We state now the CSS construction for asymmetric EAQECCs [11].

Theorem F.2.5 (CSS Construction)**.** *Let* $C_i \subset \mathbb{F}_q^n$ *be linear codes of dimension* k_i, *for* $i = 1, 2$. *Then, there is an asymmetric EAQECC with parameters* $[[n,\kappa,\delta_z/\delta_x;c]]_q$, *where*

$$c = k_1 - \dim(C_1 \cap C_2^{\perp}),\ \kappa = n - (k_1+k_2) + c,$$
$$\delta_z = \mathrm{wt}\left(C_1^{\perp} \setminus \left(C_1^{\perp} \cap C_2\right)\right) \text{ and } \delta_x = \mathrm{wt}\left(C_2^{\perp} \setminus \left(C_2^{\perp} \cap C_1\right)\right).$$

Let $\delta_z^* := \mathrm{wt}(C_1^{\perp})$ and $\delta_x^* := \mathrm{wt}(C_2^{\perp})$. If $\delta_z = \delta_z^*$ and $\delta_x = \delta_x^*$, we say that the corresponding EAQECC is *pure*, and we say it is *impure* if $\delta_z > \delta_z^*$ or $\delta_x > \delta_x^*$.

As we stated in the introduction, we are interested in constructing QECCs with a flexible amount of entanglement and, in particular, without entanglement assistance. This corresponds to pairs of codes C_1, C_2 such that $\dim \mathrm{Hull}_{C_2}(C_1) = \dim C_1$, equivalently, $C_1 \subset C_2^{\perp}$.

For the Hermitian construction, we need to consider codes defined over $\mathbb{F}_{q^2}^n$ and the Hermitian product. For two vectors $v, w \in \mathbb{F}_{q^2}^n$, their Hermitian product is

$$v \cdot_h w := \sum_{i=1}^{n} v_i w_i^q.$$

The Hermitian dual of a code $C \subset \mathbb{F}_{q^2}^n$ is defined as $C^{\perp_h} := \{v \in \mathbb{F}_{q^2}^n \mid v \cdot_h w = 0,\ \forall\, w \in C\}$.

Remark F.2.6. For a code $C \subset \mathbb{F}_{q^2}^n$, we have that $C^{\perp_h} = (C^{\perp})^q$, where we consider the component wise power of q. This implies that the Euclidean dual and the Hermitian dual codes have the same parameters.

We can state now the Hermitian construction for EAQECCs [5, 10].

Theorem F.2.7 (Hermitian construction)**.** *Let $C \subset \mathbb{F}_{q^2}^n$ be a linear code of dimension k and $C^{\perp_h}$ its Hermitian dual. Then, there is an EAQECC with parameters $[[n, \kappa, \delta; c]]_q$, where*

$$c = k - \dim(C \cap C^{\perp_h}),\ \kappa = n - 2k + c, \quad \textit{and} \quad \delta = \mathrm{wt}(C^{\perp_h} \setminus (C \cap C^{\perp_h})).$$

From the Hermitian construction for EAQECCs we can only obtain symmetric EAQECCs, that is, EAQECCs with $\delta_z = \delta_x = \delta$. Thus, if we define $\delta^* := \mathrm{wt}(C^{\perp_h})$, the corresponding quantum code is impure if $\delta > \delta^*$, and pure otherwise.

For asymmetric QECCs (EAQECCs with $c = 0$), we will use the notation $[[n, \kappa, \delta_z/\delta_x]]_q$ for their parameters. Analogously, for symmetric QECCs we will use $[[n, \kappa, \delta]]_q$. In all of our results, we compute δ_z^* and δ_x^* (δ^* respectively for the Hermitian construction), thus obtaining lower bounds for the true minimum distance of the corresponding EAQECCs.

F.3 CSS construction

In this section, we focus on the QECCs obtained using the CSS Construction F.2.5 with projective Reed-Muller codes. We do this by increasing the size of the relative hull via equivalent codes. We give some preliminaries first. Given two vectors $v, u \in \mathbb{F}_q^n$, we use the following notation:

$$u \star v := (u_1 v_1, \ldots, u_n v_n) \in \mathbb{F}_q^n.$$

For two codes C_1, C_2 in $\mathbb{F}_q^n$, we consider

$$C_1 \star C_2 := \langle u_1 \star u_2 \mid u_1 \in C_1,\ u_2 \in C_2 \rangle.$$

We say that C_1 is monomially equivalent to C_2 if there is some vector $v \in \mathbb{F}_q^n$ with Hamming weight n such that $C_1 = \langle v \rangle \star C_2$. In more generality, we will say that two codes C and C' are *equivalent* if there exists a vector $v \in \mathbb{F}_q^n$ and a permutation σ such that

$$C = \langle v \rangle \star \sigma(C').$$

It is clear that equivalent codes have the same basic parameters. Moreover, due to MacWilliam's Theorem [21], every isometry on $\mathbb{F}_q^n$ with respect to the Hamming metric can be obtained in this way for some vector $v \in \mathbb{F}_q^n$ and some permutation σ. The following result from [1] allows us to increase the dimension of the relative hull of projective Reed-Muller codes in some cases via equivalent codes.

Theorem F.3.1. *For $i = 1, 2$, let C_i be $[n, k_i]_q$ codes with $q > 2$. For any ℓ with $\max\{0, k_1 - k_2\} \leq \ell \leq \max \mathrm{wt}((C_1 \star C_2)^{\perp}) - n + k_1$, there exists a code $C_{1,\ell}$ equivalent to C_1 such that*

$$\dim \mathrm{Hull}_{C_2}(C_{1,\ell}) = \ell.$$

In particular, if $\max \mathrm{wt}((C_1 \star C_2)^{\perp}) = \min\{n, 2n - k_1 - k_2\}$, ℓ runs over all the possible values of $\dim \mathrm{Hull}_{C_2}(C_1')$, where C_1' is a code equivalent to C_1.

Remark F.3.2. For a quantum code C with parameters $[[n, \kappa, \delta; c]]_q$, the rate and net rate are defined as $\rho := \kappa/n$ and $\overline{\rho} := (\kappa - c)/n$, respectively. If this code is constructed with two codes C_1, C_2 using Theorem F.2.5, and we consider an equivalent code $C_{1,\ell}$ as in Theorem F.3.1, then the resulting quantum code has the same net rate. The same happens with codes constructed with the Hermitian construction.

The following lemma is key to study the orthogonality and will be used in the subsequent results.

Lemma F.3.3. *Let γ be a non-negative integer, and $x^\gamma \in \mathbb{F}_q[x]$. We have the following:*

$$\sum_{z\in\mathbb{F}_q} x^\gamma(z) = \begin{cases} 0 & \text{if } \gamma = 0 \text{ or } \gamma > 0 \text{ and } \gamma \not\equiv 0 \bmod (q-1), \\ -1 & \text{if } \gamma > 0 \text{ and } \gamma \equiv 0 \bmod (q-1). \end{cases}$$

Proof. Let $\xi \in \mathbb{F}_q$ be a primitive element. Then $\mathbb{F}_q = \{\xi^0, \xi^1, \ldots, \xi^{N-2}\} \cup \{0\}$. If $\gamma = 0$, $x^\gamma = 1$, and the sum is equal to $|\mathbb{F}_q| = q = 0$ in $\mathbb{F}_q$. If $\gamma > 0$ and $\gamma \equiv 0 \bmod (q-1)$, then $x^\gamma(z) = 1$ for all $z \in \mathbb{F}_q^*$, and $\sum_{z\in\mathbb{F}_q} x^\gamma(z) = q - 1 = -1$. Finally, if $\gamma > 0$ and $\gamma \not\equiv 0 \bmod (q-1)$, we have

$$\sum_{z\in\mathbb{F}_q} x^\gamma(z) = \sum_{i=0}^{q-2} (\xi^i)^\gamma = \frac{\xi^{\gamma(q-1)} - 1}{\xi^\gamma - 1} = 0.$$

□

Remark F.3.4. When working over the affine space $\mathbb{A}^\ell$, for $1 \le \ell \le m$, if we consider $x_1^{\alpha_1} \cdots x_\ell^{\alpha_\ell} \in \mathbb{F}_q[x_1, \ldots, x_m]$, we have

$$\sum_{Q\in\mathbb{A}^\ell} x_1^{\alpha_1} \cdots x_\ell^{\alpha_\ell}(Q) = \left(\sum_{z\in\mathbb{F}_q} x_1^{\alpha_1}(z)\right) \cdots \left(\sum_{z\in\mathbb{F}_q} x_\ell^{\alpha_\ell}(z)\right).$$

Thus, we can use Lemma F.3.3 in order to obtain the result of this sum. In particular, if we have $\alpha_i < q-1$ for some $1 \le i \le \ell$, this sum is equal to 0.

To increase the dimension of the hull using Theorem F.3.1, we first note that, if $C_i = \mathrm{PRM}_{d_i}(m)$, for $i = 1, 2$, then $C_1 \star C_2 = \mathrm{PRM}_{d_1+d_2}(m)$. If $k_1 + k_2 > n$, from [23, Lem. 4.8] we obtain that $\mathrm{wt}(C_1 \star C_2) = \mathrm{wt}(\mathrm{PRM}_{d_1+d_2}(m)) = 1$. By Theorem F.2.1, this implies that $d_1 + d_2 > m(q-1)$ and in that case we have $\mathrm{PRM}_{d_1+d_2}(m) = \mathbb{F}_q^n$ (see [28]). Therefore, $(C_1 \star C_2)^\perp = \{0\}$. In other words, we can only have $(C_1 \star C_2)^\perp \neq \{0\}$ if $k_1 + k_2 \le n$ for the case of projective Reed-Muller codes. If $k_1 + k_2 \le n$, then, according to Theorem F.3.1, we need to find a vector of Hamming weight n in $(C_1 \star C_2)^\perp$. This code is a projective Reed-Muller code if C_1 and C_2 are projective Reed-Muller codes (see Theorem F.2.2), which motivates the following lemma.

Lemma F.3.5. *Let $1 \le d < q-2$. Then there is a vector of Hamming weight $n = \frac{q^{m+1}-1}{q-1}$ in $\mathrm{PRM}_d^\perp(m)$.*

Proof. Let t be a monic polynomial of degree $q-1-d$ such that $t(z) \neq 0$ for every $z \in \mathbb{F}_q$. For example, we can choose t as a monic irreducible polynomial in $\mathbb{F}_q[x]$. We consider the vector $v = (v_Q)_{Q\in P^m} \in \mathbb{F}_q^n$ defined in the following way: if $Q = (0, 0, \ldots, 0, 1, z)$, for some $z \in \mathbb{F}_q$, we define $v_Q = t(z)$, and $v_Q = 1$ otherwise. For $0 \le i \le q-1-d$, let t_i be the coefficient of x^i in t. We consider the following decomposition of $P^m =$

$(\{1\} \times \mathbb{F}_q^m) \cup (\{0\} \times \{1\} \times \mathbb{F}_q^{m-1}) \cup \cdots \cup \{(0,0,\ldots,0,1)\} = B_m \cup B_{m-1} \cup \cdots \cup B_0$. Let $x_0^{\alpha_0} x_1^{\alpha_1} \cdots x_m^{\alpha_m} = x^\alpha \in \mathbb{F}_q[x_0,\ldots,x_m]_d$. Then we have

$$v \cdot \mathrm{ev}(x^\alpha) = \sum_{Q \in B_m} v_Q x^\alpha(Q) + \sum_{Q \in B_{m-1}} v_Q x^\alpha(Q) + \cdots + \sum_{Q \in B_0} v_Q x^\alpha(Q).$$

For $2 \leq i \leq m$, we have $v_Q = 1$ and

$$\sum_{Q \in B_i} v_Q x^\alpha(Q) = \sum_{Q \in B_i} x^\alpha(Q) = 0$$

by Lemma F.3.3 and Remark F.3.4 because $\alpha_j < q-1$ for $0 \leq j \leq m$.

We study the sum over B_1 now. If $\alpha_j = 0$ for every $0 \leq j \leq m-2$, we have

$$\sum_{Q=(0,0,\ldots,1,z) \in B_1} v_Q x^\alpha(Q) = \sum_{z \in \mathbb{F}_q} t(z) x_m^{\alpha_m}(z) = \sum_{l=0}^{q-1-d} t_l \sum_{z \in \mathbb{F}_q} x_m^{\alpha_m + l}(z). \tag{F.3.1}$$

Taking into account that $\alpha_m \leq d$, we have $\alpha_m + l \leq q-1$, and we can only have the equality for some $l \in \{0,\ldots,q-1-d\}$ if $\alpha_m = d$. Therefore, by Lemma F.3.3, this sum is equal to 0 unless $\alpha_m = d$, in which case it is equal to $-t_{q-1-d} = -1$ (t is monic).

On the other hand, if we have $\alpha_j > 0$ for some $0 \leq j \leq m-2$, then the sum over B_1 in (F.3.1) is clearly equal to 0 because all the addends are equal to 0. For the sum over B_0, it is clear that this sum is equal to 0 unless $\alpha_m = d$, in which case it is equal to 1. Hence, if $\alpha_m \neq d$, all the sums are equal to 0 and we have $v \cdot \mathrm{ev}(x^\alpha) = 0$, and if $\alpha_m = d$, all the sums are 0 besides the sums corresponding to B_1 and B_0, which are equal to -1 and 1, respectively. Thus, if $\alpha_m = d$ we also have $v \cdot \mathrm{ev}(x_m^d) = 0$. This implies that $v \in \mathrm{PRM}_d^\perp(m)$, and the fact that v has Hamming weight n follows from its definition. □

Note that, for $d \equiv 0 \bmod q-1$, $d \leq \lfloor m(q-1)/2 \rfloor$, we have $(1,\ldots,1)$ in $\mathrm{PRM}_d^\perp(m)$ by Theorem F.2.2, which is a vector of Hamming weight n, and we also know that the corresponding projective Reed-Muller code is contained in its dual [26, Cor. 10.3]. As a consequence of Theorem F.3.1 and Lemma F.3.5, we obtain the following.

Proposition F.3.6. *Let $q > 2$ and let $1 \leq d_1 \leq d_2 < q-2$. Let $C_i = \mathrm{PRM}_{d_i}(m)$, for $i = 1,2$. If $d_1 + d_2 < q-2$, then, for any $0 \leq \ell \leq \dim C_1$, there is a code $C_{1,\ell}$ monomially equivalent to C_1 such that*

$$\dim C_{1,\ell} \cap C_2^\perp = \ell.$$

Proof. We have that $C_1 \star C_2 = \mathrm{PRM}_{d_1+d_2}(m)$, with $d_1 + d_2 < q-2$. By Lemma F.3.5, there is a vector of Hamming weight n in $(C_1 \star C_2)^\perp$. Using Theorem F.3.1, we obtain the result. □

We can use Proposition F.3.6 and Theorem F.2.5 to construct asymmetric and symmetric QECCs. The following result, for the case $m = 2$, allows us to vary the parameter c from the codes arising in [24], thus giving more flexible parameters.

Theorem F.3.7. *Let $1 \leq d_1 \leq d_2 < q-2$ such that $d_1 + d_2 < q-2$. Then we can construct a quantum code with parameters $[[n, \kappa + c, \delta_z/\delta_x; c]]_q$, for any $0 \leq c \leq \dim \mathrm{PRM}_{d_1}(m)$, where $n = \frac{q^{m+1}-1}{q-1}$, $\kappa = n - (\dim \mathrm{PRM}_{d_1}(m) + \dim \mathrm{PRM}_{d_2}(m))$, $\delta_z \geq \mathrm{wt}(\mathrm{PRM}_{d_2}^\perp(m))$ and $\delta_x \geq \mathrm{wt}(\mathrm{PRM}_{d_1}^\perp(m))$.*

The previous result can be used to obtain QECCs that outperform affine Reed-Muller codes, as the next example shows.

Remark F.3.8. For $1 \leq d_1 \leq d_2 < q-2$ such that $d_1 + d_2 < q-2$, by Theorem F.2.3 and Theorem F.2.1 (or directly by counting monomials in m variables of degree $\leq d$ and monomials of degree d in $m+1$ variables) we have $\dim \mathrm{RM}_{d_i}(m) = \sum_{t=0}^{d_i} \binom{t+m-1}{t} = \binom{d_i+m}{m} = \dim \mathrm{PRM}_{d_i}(m)$, for $i = 1, 2$. Moreover, we have that $\mathrm{wt}(\mathrm{PRM}_{d_i}^{\perp}(m)) = \mathrm{wt}(\mathrm{PRM}_{d_i^{\perp}}(m)) = \mathrm{wt}(\mathrm{RM}_{d_i^{\perp}-1}(m)) = \mathrm{wt}(\mathrm{RM}_{d_i}^{\perp}(m))$, where $d_i^{\perp} = m(q-1) - d_i$, for $i = 1, 2$. Therefore, using Theorem F.2.5 with $C_i = \mathrm{RM}_{d_i}(m)$ for $i = 1, 2$, we get an asymmetric QECC with parameters

$$[[q^m, q^m - (\dim \mathrm{RM}_{d_1}(m) + \dim \mathrm{RM}_{d_2}(m)), \mathrm{wt}(\mathrm{RM}_{d_2}^{\perp}(m))/\mathrm{wt}(\mathrm{RM}_{d_1}^{\perp}(m))]]_q.$$

On the other hand, using Theorem F.3.7 with $c = 0$ we can get an asymmetric QECC with parameters

$$[[q^m + \Delta, q^m + \Delta - (\dim \mathrm{PRM}_{d_1}(m) + \dim \mathrm{PRM}_{d_2}(m)), \mathrm{wt}(\mathrm{PRM}_{d_2}^{\perp}(m))/\mathrm{wt}(\mathrm{PRM}_{d_1}^{\perp}(m))]]_q,$$

where $\Delta = \frac{q^m-1}{q-1}$. Taking into account the previous discussion, we see that both asymmetric QECCs have the same minimum distances δ_z and δ_x, but the code obtained using Theorem F.3.7 has gained Δ units in length and dimension, which increases the code rate and decreases the relative minimum distances. If we consider $\frac{\kappa+\delta_z}{n}$ (resp. $\frac{\kappa+\delta_x}{n}$) as a measure of how good a code is in terms of transmission rate and phase-shift error-correction capability (resp. qudit-flip error-correction capability), we see that in this case we obtain asymmetric QECCs with better performance using projective Reed-Muller codes (Theorem F.3.7) than the asymmetric QECCs obtained using affine Reed-Muller codes.

The quantum Gilbert-Varshamov bound from [22] can be used to check the goodness of the parameters of an asymmetric QECC.

Theorem F.3.9. *Assume the existence of integers $n \geq 1$, $1 \leq l < n + c$, $\delta_x \geq 1$, $\delta_z \geq 1$, $0 \leq c \leq l/2$ such that*

$$\frac{q^{2n-l} - q^{l-2c}}{q^{2n} - 1} \left(\sum_{i=0}^{\delta_x - 1} \binom{n}{i} (q-1)^i \sum_{j=0}^{\delta_z - 1} \binom{n}{j} (q-1)^j - 1 \right) < 1.$$

Then there is an EAQECC with parameters $[[n, n-l+c, \delta_z/\delta_x; c]]_q$.

Given a quantum Gilbert-Varshamov bound, like that one from Theorem F.3.9, we will say that a code C surpasses it if the bound does not guarantee the existence of a code with the parameters of C.

Example F.3.10. Let $q = 8$, $m = 2$, $d_1 = 1$ and $d_2 = 4$. We have $d_1 + d_2 = 5 < q - 2$, and we can apply Theorem F.3.7 to obtain QECCs with parameters $[[73, 55 + c, 6/3; c]]_8$, for $0 \leq c \leq \dim \mathrm{PRM}_1(2) = 3$. All of these codes surpass the Gilbert-Varshamov bound from Theorem F.3.9.

In some cases it is possible to obtain nested pairs of codes from subfield subcodes of projective Reed-Muller codes, giving rise to QECCs, as we show in the next result.

Proposition F.3.11. *Let d_1, d_2 such that $d_1 + d_2 = \lambda(q^s - 1)$, with $1 \leq \lambda \leq m$. Then we have $(\mathrm{PRM}_{d_1}(q^s, m))_q \subset ((\mathrm{PRM}_{d_2}(q^s, m))_q)^\perp$, and we can construct a QECC with parameters $[[n, \kappa, \delta_z/\delta_x]]_q$, where $n = \frac{q^{s(m+1)}-1}{q^s-1}$, $\kappa = n - \dim(\mathrm{PRM}_{d_1}(q^s, m))_q - \dim(\mathrm{PRM}_{d_2}(q^s, m))_q$, $\delta_z \geq \mathrm{wt}(((\mathrm{PRM}_{d_2}(q^s, m))_q)^\perp)$ and $\delta_x \geq \mathrm{wt}(((\mathrm{PRM}_{d_1}(q^s, m))_q)^\perp)$.*

Proof. By hypothesis we have $d_1 \equiv d_2^\perp \bmod q^s - 1$ and $d_1 \leq d_2^\perp$. By [26, Lem. 10.7], $\mathrm{PRM}_{d_1}(q^s, m) \subset \mathrm{PRM}^\perp_{d_2}(q^s, m)$. This implies

$$(\mathrm{PRM}_{d_1}(q^s, m))_q \subset (\mathrm{PRM}^\perp_{d_2}(q^s, m))_q \subset ((\mathrm{PRM}_{d_2}(q^s, m))_q)^\perp.$$

The parameters follow from Theorem F.2.5. □

Remark F.3.12. In general, we do not know $\mathrm{wt}(((\mathrm{PRM}_{d_i}(q^s, m))_q)^\perp)$, for $i = 1, 2$. Nevertheless, we can compute this minimum distance with Magma [4]. In some cases, the code $(\mathrm{PRM}_{d_i}(q^s, m))_q$ can be degenerate, that is, its generator matrix has a column of zeroes. In that case, the minimum distance of its dual is equal to 1. This problem can easily be avoided by considering the results from [25], where some particular degrees are considered such that $(\mathrm{PRM}_{d_i}(q^s, m))_q$ is nondegenerate. For those degrees, the resulting codes have good parameters and we have formulas for the dimension of the subfield subcode (for the case $m = 2$, one can also use the results from [14] for the dimension). In the next example, we show how to use those results together with Proposition F.3.11.

Example F.3.13. Let $m = 2 = s$. From [25] (or [14]), if $d_i \equiv 0 \bmod (q^s - 1)/(q - 1)$, then $(\mathrm{PRM}_{d_i}(q^s, 2))_q$ is non degenerate, for $i = 1, 2$. If we set $q = 2$, from Proposition F.3.11 we obtain a code with parameters $[[73, 19, 9/9]]_2$ with $d_1 = d_2 = 7$. For $q = 3$, we obtain the parameters $[[91, 73, 4/4]]_3$ with $d_1 = d_2 = 4$, and $[[91, 12, 36/4]]_2$ with $d_1 = 4$, $d_2 = 12$. All of them surpass the Gilbert-Varshamov bound from Theorem F.3.9.

F.4 Hermitian construction

In the Hermitian case, we can also obtain quantum codes with projective Reed-Muller codes without entanglement assistance. Recall that in this case we have to consider codes over $\mathbb{F}_{q^2}$ and the Hermitian product. The following result from [7, Thm. 2.1] is analogous in part to Theorem F.3.1 for the Hermitian product.

Theorem F.4.1. *Let $C \subset \mathbb{F}_{q^2}$ be a linear code. If there is a vector $v \in ((C \star C^q)^\perp)_q$ with $\mathrm{wt}(v) = n$, then $\langle v \rangle \star C \subset (\langle v \rangle \star C)^{\perp_h}$, i.e., $\langle v \rangle \star C$ is self-orthogonal with respect to the Hermitian product.*

Note that, unlike Theorem F.3.1, the previous result does not cover all the possible values of the dimension of the Hermitian hull, we go directly to the case $\mathrm{Hull}_H(C) = C$. The rest of the values are covered by the following result from [20].

Theorem F.4.2. *Let $q > 2$ and let $C \subset \mathbb{F}_{q^2}^n$ with $\dim \mathrm{Hull}_H(C) = \ell$. Then there exists a monomially equivalent code $C_{\ell'}$ with $\dim \mathrm{Hull}_H(C_{\ell'}) = \ell'$, for each $0 \leq \ell' \leq \ell$.*

Therefore, using Theorem F.4.1 and Theorem F.4.2, if we find a vector $v \in ((C \star C^q)^\perp)_q$ with $\mathrm{wt}(v) = n$, then we can find an equivalent code C_ℓ such that $\dim \mathrm{Hull}_H(C_\ell) = \ell$, for $0 \leq \ell \leq \dim C$, if $q > 2$.

With respect to projective Reed-Muller codes, we start by determining some of these codes which are self-orthogonal with respect to the Hermitian product, without considering equivalent codes.

Proposition F.4.3. *Let $d = \lambda(q-1)$ with $1 \leq \lambda \leq m$. Then $\mathrm{PRM}_d(q^2, m) \subset \mathrm{PRM}_d^{\perp_h}(q^2, m)$. As a consequence, if $d \equiv 0 \bmod q-1$ and $d \not\equiv 0 \bmod q^2-1$, we can construct a QECC with parameters $[[n, \kappa, \delta]]_q$, where $n = \frac{q^{2(m+1)}-1}{q^2-1}$, $\kappa = n - 2(\dim \mathrm{PRM}_d(q^2, m))$ and $\delta \geq \mathrm{wt}(\mathrm{PRM}_d^{\perp}(q^2, m))$.*

Proof. We have

$$((\mathrm{PRM}_d(q^2, m) \star \mathrm{PRM}_d(q^2, m)^q)^{\perp})_q \supset (\mathrm{PRM}_{d+qd}^{\perp}(q^2, m))_q.$$

By Theorem F.2.2, if we have $d(q+1) \equiv 0 \bmod q^2-1$, with $d(q+1) \leq m(q^2-1)$, then $(1, \ldots, 1) \in (\mathrm{PRM}_{d+qd}^{\perp}(q^2, m))_q$ and we can apply Theorem F.4.1 with $C = \mathrm{PRM}_d(q^2, m)$. The parameters of the quantum code are deduced from Theorems F.2.1, F.2.2 and F.2.7. □

With this construction (and, in general, with the results of this section) we manage to construct very long codes over small finite field sizes. To check the performance of these codes, we introduce now another quantum Gilbert-Varshamov bound from [9], which seems to be more difficult to surpass for symmetric QECCs than the bound from Theorem F.3.9.

Theorem F.4.4. *Suppose that $n > \kappa$, $\delta \geq 2$ and $n \equiv \kappa \bmod 2$. Then there exists a pure stabilizer quantum code $[[n, \kappa, \delta]]_q$, provided that*

$$\frac{q^{n-\kappa+2}-1}{q^2-1} > \sum_{i=1}^{\delta-1} (q^2-1)^{i-1} \binom{n}{i}.$$

Example F.4.5. Let $q = 2$ and $m = 3$. For $d = q-1 = 1$ we can apply Proposition F.4.3 to obtain a QECC with parameters $[[85, 77, 3]]_2$, which is optimal according to [15]. For $m = 4$, we get a QECC with parameters $[[341, 331, 3]]_2$.

Consider now $q = 3$ and $d = q-1 = 2$. For $m = 2$, we obtain the parameters $[[91, 79, 4]]_3$, and for $m = 3$ we obtain $[[820, 800, 4]]_3$. All the codes in this example surpass the quantum Gilbert-Varshamov bound from Theorem F.4.4.

When $d \not\equiv 0 \bmod q-1$, we can use Theorems F.4.1 and F.4.2 to construct quantum codes with a variable amount of entanglement using equivalent codes in some cases. The idea of the proof of the following result can be regarded as an extension of the proof from [2, Thm. 4] for projective Reed-Solomon codes.

Theorem F.4.6. *Let $1 \leq d < q-2$. Then we can construct an EAQECC with parameters $[[n, \kappa + c, \delta; c]]_q$, for any $0 \leq c \leq \dim \mathrm{PRM}_d(q^2, m)$, where $n = \frac{q^{2(m+1)}-1}{q^2-1}$, $\kappa = n - 2(\dim \mathrm{PRM}_d(q^2, m))$ and $\delta \geq \mathrm{wt}(\mathrm{PRM}_{d^{\perp}}(q^2, m))$.*

Proof. We use Theorems F.4.1 and F.4.2 with $C = \mathrm{PRM}_d(q^2, m)$. First, we find $w \in ((C \star C^q)^{\perp})_q$ with $\mathrm{wt}(v) = n$. Let t be a monic polynomial with coefficients in $\mathbb{F}_{q^2}$ of degree $q-1-d$ such that $t(z) \neq 0$ for every $z \in \mathbb{F}_{q^2}$, and $v \in \mathbb{F}_{q^2}^n$ as in Lemma F.3.5. Then we consider $w := v^{q+1}$, where the power is taken component wise. Clearly $w \in \mathbb{F}_q^n$,

$\mathrm{wt}(w) = n$, and we will prove that $w \in (C \star C^q)^\perp$. Let $x^\alpha, x^\beta \in \mathbb{F}_{q^2}[x_0, \ldots, x_m]_d$. Using the decomposition $P^m = B_m \cup B_{m-1} \cup \cdots \cup B_0$ from the proof of Lemma F.3.5 we have that

$$w \cdot (\mathrm{ev}(x^\alpha) \star \mathrm{ev}(x^{q\beta})) = \sum_{i=0}^{m} \sum_{Q \in B_i} v_Q^{q+1} x^{\alpha+q\beta}(Q).$$

For $2 \leq i \leq m$, we have $v_Q = 1$ and

$$\sum_{Q \in B_i} v_Q^{q+1} x^{\alpha+q\beta}(Q) = \sum_{Q \in B_i} x^{\alpha+q\beta}(Q) = 0$$

because $\alpha_j + q\beta_j < q - 1 + q(q-1) = q^2 - 1$ for $0 \leq j \leq m$.

On the other hand, if $\alpha_j = 0$ for $0 \leq j \leq m-2$, we have

$$\sum_{Q=(0,0,\ldots,1,z) \in B_1} v_Q^{q+1} x^{\alpha+q\beta}(Q) = \sum_{z \in \mathbb{F}_{q^2}} t(z)^{q+1} z^{\alpha_m + q\beta_m} = \sum_{l=0}^{(q+1)(q-1-d)} r_l \sum_{z \in \mathbb{F}_{q^2}} z^{l+\alpha_m+q\beta_m}, \tag{F.4.1}$$

where r_l is the coefficient of x^l in t^{q+1}. Taking into account that $l + \alpha_m + q\beta_m \leq (q+1)(q-1-d) + d + qd = q^2 - 1$, we see that this sum is equal to 0 unless $\alpha_m = \beta_m = d$, in which case it is equal to $-r_{(q+1)(q-1-d)} = -1$ (since t is monic), because of Lemma F.3.3 and Remark F.3.4. If we have $\alpha_j > 0$ for some $0 \leq j \leq m-2$, then all the addends in (F.4.1) are equal to 0. For the sum over B_0, it is clear that this sum is equal to 0 unless $\alpha_m = \beta_m = d$, in which case it is equal to 1.

Therefore, if $\alpha_m \neq d$ or $\beta_m \neq d$, all the sums are equal to 0 and we have $w \cdot (\mathrm{ev}(x^\alpha) \star \mathrm{ev}(x^{q\beta})) = 0$, and if $\alpha_m = \beta_m = d$, all the sums are 0 besides the sums corresponding to B_1 and B_0, which are equal to -1 and 1, respectively. Thus, if $\alpha_m = \beta_m = d$ we also have $w \cdot (\mathrm{ev}(x^\alpha) \star \mathrm{ev}(x^{q\beta})) = 0$. This implies that $w \in (C \star C^q)^\perp$. Therefore, $\langle w \rangle \star C \subset (\langle w \rangle \star C)^{\perp_h}$ by Theorem F.4.1, and we finish the proof by applying the Hermitian construction from Theorem F.2.7 to $\langle w \rangle \star C$ and considering Theorem F.4.2. □

The argument in Remark F.3.8, changing q with q^2 and $d_1 = d_2 = d$ (note that $d < q-2$ implies $2d < q^2 - 2$), shows that, using the QECCs from Theorem F.4.6, we can obtain QECCs with $\frac{q^{2m}-1}{q^2-1}$ extra length and dimension with respect to the affine case. In the next example, we show some codes obtained from Theorem F.4.6 with good parameters.

Example F.4.7. We consider $q = 4$ and $m = 2$. Therefore, we work over the field $\mathbb{F}_{4^2}$ and we obtain codes of length $\frac{q^{2(m+1)}-1}{q^2-1} = 273$. For $d = 1$ we can apply Theorem F.4.6 to obtain a QECC with parameters $[[273, 267, 3]]_4$. This code improves the parameters of the code $[[273, 265, 3]]_4$ from [3] and surpasses the quantum Gilbert-Varshamov from Theorem F.4.4.

For $q = 5$, $m = 2$ and $d = 1, 2$, we obtain the parameters $[[651, 645, 3]]_5$ and $[[651, 639, 4]]_5$, respectively. The first one improves the parameters $[[651, 642, 3]]_5$ and $[[652, 644, 3]]_5$ obtained in [3], and the second one improves the parameters $[[651, 636, 4]]_5$ and $[[652, 638, 4]]_5$ from [3]. Both of them exceed the quantum Gilbert-Varshamov bound from Theorem F.4.4.

Similarly to the previous section, we can also use subfield subcodes of projective Reed-Muller codes in some cases. For the Hermitian product, we consider projective Reed-Muller codes over $\mathbb{F}_{q^{2s}}$ such that their subfield subcodes with respect to the extension $\mathbb{F}_{q^{2s}}/\mathbb{F}_{q^2}$ are self-orthogonal with respect to the Hermitian product, which gives rise to QECCs over $\mathbb{F}_q$ using the Hermitian construction from Theorem F.2.7.

Proposition F.4.8. *Let $d = \lambda(q^{2s}-1)/(q+1)$ with $1 \leq \lambda \leq m$. Then $(\mathrm{PRM}_d(q^{2s}, m))_{q^2} \subset ((\mathrm{PRM}_d(q^{2s}, m))_{q^2})^{\perp_h}$. As a consequence, we can construct a QECC with parameters $[[n, \kappa, \delta]]_q$, where*

$$n = \frac{q^{2s(m+1)} - 1}{q^{2s} - 1},\ \kappa = n - 2(\dim(\mathrm{PRM}_d(q^{2s}, m))_{q^2})\ \text{and}\ \delta \geq \mathrm{wt}(((\mathrm{PRM}_d(q^{2s}, m))_{q^2})^{\perp}).$$

Proof. We have

$$\begin{aligned}(((\mathrm{PRM}_d(q^{2s}, m))_{q^2} \star ((\mathrm{PRM}_d(q^{2s}, m))_{q^2})^q)^{\perp})_q &\supset ((\mathrm{PRM}_d(q^{2s}, m) \star (\mathrm{PRM}_d(q^{2s}, m))^q)^{\perp})_q \\ &\supset (\mathrm{PRM}^{\perp}_{d+qd}(q^{2s}, m))_q.\end{aligned}$$

The rest of the proof follows as in the proof of Proposition F.4.3, changing q^2 with q^{2s}. □

As we stated in Remark F.3.12, we can use the results from [25] to obtain QECCs with good parameters, whose minimum distance can be computed using Magma [4]. We show this in the next example.

Example F.4.9. By [25, Cor. 4.1 and Cor 4.2], if $d \equiv 0 \bmod (q^{2s}-1)/(q^2-1)$, then we have recursive formulas for the dimension of $(\mathrm{PRM}_d(q^{2s}, m))_{q^2}$, and we know that $(\mathrm{PRM}_d(q^{2s}, m))_{q^2}$ is non degenerate (this is also seen recursively, using what we know for the case $m = 1$ from [13]).

Let $q = 2$ and $m \geq 2$. Then $(q^{2s}-1)/(q+1) = (q^{2s}-1)/(q^2-1) = (4^s-1)/3$. Hence, by Proposition F.4.8, if we consider $d = \lambda(4^s-1)/3$, for some $1 \leq \lambda \leq m$, then we have $(\mathrm{PRM}_d(4^s, m))_{q^2} \subset ((\mathrm{PRM}_d(4^s, m))_{q^2})^{\perp_h}$, and by the previous discussion $((\mathrm{PRM}_d(4^s, m))_{q^2})^{\perp_h}$ is non degenerate. For example, for $m = s = 2$, we can consider $\lambda = 1$ and $d = 5$. The corresponding quantum code has parameters $[[273, 255, 4]]_2$, which improves the parameters $[[274, 248, 4]]_2$ and $[[273, 246, 4]]_2$ from [3]. If we consider $m = 3$ instead, we obtain the parameters $[[4369, 4337, 4]]_2$. Both of the codes surpass the Gilbert-Varshamov bound from Theorem F.4.4.

Remark F.4.10. If $q > 2$, one can also use Theorem F.4.2 with Proposition F.4.3 or Proposition F.4.8 to obtain EAQECCs with a variable amount of entanglement.

Bibliography

[1] S. E. Anderson, E. Camps-Moreno, H. H. López, G. L. Matthews, D. Ruano, and I. Soprunov. Relative hulls and quantum codes. *IEEE Trans. Inform. Theory*, 70(5):3190–3201, 2024.

[2] S. Ball. Some constructions of quantum MDS codes. *Des. Codes Cryptogr.*, 89(5):811–821, 2021.

[3] J. Bierbrauer and Y. Edel. Quantum twisted codes. *J. Combin. Des.*, 8(3):174–188, 2000.

[4] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[5] T. Brun, I. Devetak, and M.-H. Hsieh. Correcting quantum errors with entanglement. *Science*, 314(5798):436–439, 2006.

[6] A. R. Calderbank and P. W. Shor. Good quantum error-correcting codes exist. *Phys. Rev. A*, 54:1098–1105, Aug 1996.

[7] H. Chen. On the hull-variation problem of equivalent linear codes. *IEEE Trans. Inform. Theory*, 69(5):2911–2922, 2023.

[8] P. Delsarte, J.-M. Goethals, and F. J. MacWilliams. On generalized Reed-Muller codes and their relatives. *Information and Control*, 16:403–442, 1970.

[9] K. Feng and Z. Ma. A finite Gilbert-Varshamov bound for pure stabilizer quantum codes. *IEEE Trans. Inform. Theory*, 50(12):3323–3325, 2004.

[10] C. Galindo, F. Hernando, R. Matsumoto, and D. Ruano. Entanglement-assisted quantum error-correcting codes over arbitrary finite fields. *Quantum Inf. Process.*, 18(4):Paper No. 116, 18, 2019.

[11] C. Galindo, F. Hernando, R. Matsumoto, and D. Ruano. Asymmetric entanglement-assisted quantum error-correcting codes and bch codes. *IEEE Access*, 8:18571–18579, 2020.

[12] S. R. Ghorpade and R. Ludhani. On the minimum distance, minimum weight codewords, and the dimension of projective Reed-Muller codes. *Adv. Math. Commun.*, 18(2):360–382, 2024.

[13] P. Gimenez, D. Ruano, and R. San-José. Entanglement-assisted quantum error-correcting codes from subfield subcodes of projective Reed-Solomon codes. *Comput. Appl. Math.*, 42(8):Paper No. 363, 31, 2023.

[14] P. Gimenez, D. Ruano, and R. San-José. Subfield subcodes of projective Reed-Muller codes. *Finite Fields Appl.*, 94:Paper No. 102353, 46, 2024.

[15] M. Grassl. Bounds on the minimum distance of linear codes and quantum codes. Online available at `http://www.codetables.de`, 2007. Accessed on 2023-04-04.

[16] L. Ioffe and M. Mézard. Asymmetric quantum error-correcting codes. *Phys. Rev. A*, 75:032345, Mar 2007.

[17] T. Kasami, S. Lin, and W. W. Peterson. New generalizations of the Reed-Muller codes. I. Primitive codes. *IEEE Trans. Inform. Theory*, IT-14:189–199, 1968.

[18] A. Ketkar, A. Klappenecker, S. Kumar, and P. K. Sarvepalli. Nonbinary stabilizer codes over finite fields. *IEEE Trans. Inform. Theory*, 52(11):4892–4914, 2006.

[19] G. Lachaud. The parameters of projective Reed-Muller codes. *Discrete Math.*, 81(2):217–221, 1990.

[20] G. Luo, M. F. Ezerman, M. Grassl, and S. Ling. Constructing quantum error-correcting codes that require a variable amount of entanglement. *Quantum Inf. Process.*, 23(1):Paper No. 4, 28, 2024.

[21] J. MacWilliams. Error-correcting codes for multiple-level transmission. *Bell System Tech. J.*, 40:281–308, 1961.

[22] R. Matsumoto. Improved Gilbert–Varshamov bound for Entanglement-Assisted Asymmetric Quantum Error Correction by Symplectic Orthogonality. *IEEE Trans. Quantum Eng.*, 1:1–4, 2020.

[23] H. Randriambololona. On products and powers of linear codes under componentwise multiplication. In *Algorithmic arithmetic, geometry, and coding theory*, volume 637 of *Contemp. Math.*, pages 3–78. Amer. Math. Soc., Providence, RI, 2015.

[24] D. Ruano and R. San-José. Hulls of projective Reed-Muller codes over the projective plane. *SIAM Journal on Applied Algebra and Geometry, to appear. ArXiv 2312.13921*, 2024.

[25] R. San-José. A recursive construction for projective Reed-Muller codes. *IEEE Transactions on Information Theory, to appear. ArXiv 2312.05072*, 2024.

[26] P. K. Sarvepalli, S. A. Aly, and A. Klappenecker. Nonbinary stabilizer codes. In *Mathematics of quantum computation and quantum technology*, Chapman & Hall/CRC Appl. Math. Nonlinear Sci. Ser., pages 287–308. Chapman & Hall/CRC, Boca Raton, FL, 2008.

[27] P. K. Sarvepalli, A. Klappenecker, and M. Rötteler. Asymmetric quantum codes: constructions, bounds and performance. *Proc. R. Soc. Lond. Ser. A Math. Phys. Eng. Sci.*, 465(2105):1645–1672, 2009.

[28] A. B. Sørensen. Projective Reed-Muller codes. *IEEE Trans. Inform. Theory*, 37(6):1567–1576, 1991.

[29] A. Steane. Multiple-Particle Interference and Quantum Error Correction. *Proceedings of the Royal Society of London Series A*, 452(1954):2551–2577, Nov. 1996.

Paper G

An algebraic characterization of binary CSS-T codes and cyclic CSS-T codes for quantum fault tolerance

Eduardo Camps-Moreno, Hiram H. López, Gretchen L. Matthews, Diego Ruano, Rodrigo San-José, Ivan Soprunov

Abstract

CSS-T codes were recently introduced as quantum error-correcting codes that respect a transversal gate. A CSS-T code depends on a CSS-T pair, which is a pair of binary codes (C_1, C_2) such that C_1 contains C_2, C_2 is even, and the shortening of the dual of C_1 with respect to the support of each codeword of C_2 is self-dual. In this paper, we give new conditions to guarantee that a pair of binary codes (C_1, C_2) is a CSS-T pair. We define the poset of CSS-T pairs and determine the minimal and maximal elements of the poset. We provide a propagation rule for nondegenerate CSS-T codes. We apply some main results to Reed-Muller, cyclic, and extended cyclic codes. We characterize CSS-T pairs of cyclic codes in terms of the defining cyclotomic cosets. We find cyclic and extended cyclic codes to obtain quantum codes with better parameters than those in the literature.

Keywords: CSS-T construction, Schur product of linear codes, Cyclic codes, Quantum codes.

MSC: 94B05, 81P70, 11T71, 14G50.

DOI: 10.1007/s11128-024-04427-5

Reference: E. Camps-Moreno, H.H. López, G.L. Matthews, D. Ruano, R. San-José, I. Soprunov. An algebraic characterization of binary CSS-T codes and cyclic CSS-T codes for quantum fault tolerance. Quantum Inf. Process. 23, 230 (2024).

Affiliation: Eduardo Camps-Moreno, Hiram H. López, Gretchen L. Matthews: Virginia Tech. Diego Ruano, Rodrigo San-José: IMUVA-Mathematics Research Institute, Universidad de Valladolid. Ivan Soprunov: Cleveland State University.

G.1 Introduction

The development of large-scale, reliable quantum computing relies on quantum error correction to guard against the adverse impact of noise and decoherence. Quantum error-correcting codes were first discovered by Shor in 1995 [22]. Soon after that, independent works by Calderbank and Shor [8] and Steane [23] outlined how classical linear codes could be used to construct quantum error-correcting codes, now referred to as CSS codes. The CSS construction uses a pair (C_1, C_2) of classical linear codes, where the code C_1 contains the code C_2, to define a quantum stabilizer code. CSS codes are advantageous because they allow one to combine two appropriate classical codes into a quantum stabilizer code. CSS codes have some nice properties, including propagation rules (see [7, 14, 19] and the survey [13]).

While generally not optimal, CSS codes are optimal among nondegenerate stabilizer codes that support the transversal T gate; indeed it is demonstrated in [21] that for any non-degenerate stabilizer code that supports a physical transversal T gate, there is a CSS code with the same parameters that also does. CSS-T codes, introduced in [20], are motivated by the need for quantum codes which respect the transversal T gate. Transversal gates are essential in fault-tolerant quantum computation as they mitigate the proliferation of errors. Transversals may be considered the most straightforward fault-tolerant realizations because they split into gates that act on individual qubits.

A CSS-T code is formed using a pair (C_1, C_2) of classical linear codes such that C_1 contains C_2, all codewords of C_2 are of even weight, and the shortening of the dual of C_1 with respect to the support of each codeword c of C_2 is self-dual. In this case, we say that (C_1, C_2) is a CSS-T pair. It is not surprising that it remains an open question to determine asymptotically good families of CSS-T codes [4]. CSS-T codes from Reed-Muller codes have been explored in [2], and some general properties are laid out in [4].

In this paper, we study binary CSS-T pairs. Section G.2 introduces the basic properties of CSS-T pairs. We give in Theorem G.2.3 several conditions to determine if a pair of codes (C_1, C_2) is a CSS-T pair. The equivalences of Theorem G.2.3 allow us to see that the minimum distance of a CSS-T code associated with (C_1, C_2) is lower bounded by the minimum distance of $C_2^{\perp}$. In Section G.3, Corollary G.3.1 allows us to define a poset $\mathcal{P}$ of CSS-T pairs relative to the order $(C_1, C_2) \leq (C_1', C_2')$ if and only if $C_i \subset C_i'$ for $i = 1, 2$. We determine the minimal elements of $\mathcal{P}$ in Corollary G.3.3. Using a sequence of results on properties of CSS-T pairs, we provide in Corollary G.3.9 a propagation rule for nondegenerate CSS-T codes and characterize the maximal elements of $\mathcal{P}$ in Theorem G.3.11. In Corollary G.3.13, we collect special cases when the conditions of Theorem G.3.11 can be relaxed. As an application, we apply some results of Section G.3 to Reed-Muller codes. In Section G.4, we restrict our attention to cyclic and extended cyclic codes. Theorem G.4.8 provides a characterization of cyclic CSS-T pairs in terms of the defining cyclotomic cosets, and Corollary G.4.11 characterizes those that are maximal. We find cyclic and extended cyclic codes that outperform binary Reed-Muller codes. In Section G.5 we compare our codes with triorthogonal codes [6, 17]. A summary and open problems are included in Section G.6. Examples are provided throughout the paper. We conclude this section with a summary of results and a motivating example.

G.1.1 Summary of major results

In this subsection, we provide a guide to the major results of this paper.

- A primary contribution of this paper is the following more straightforward characterization of CSS-T pairs, found in Theorem G.2.3: Given binary linear codes C_1 and C_2 of length n,

  $$(C_1, C_2) \text{ is a CSS-T pair if and only if } C_2 \subset C_1 \cap (C_1^{\star 2})^{\perp}.$$

  Among the consequences are the fact that

  $$C_2 \text{ is self-orthogonal for all CSS-T pairs } (C_1, C_2).$$

- Another key result is that CSS-T pairs form a poset $\mathcal{P}$. According to Corollary G.3.1, given a CSS-T pair (C_1, C_2)

  $$(C_1', C_2) \text{ is a CSS-T pair } \forall\ C_2 \subset C_1' \subset C_1$$

  and

  $$(C_1, C_2') \text{ is a CSS-T pair } \forall\ C_2' \subset C_2.$$

- We demonstrate in Theorem G.3.11 that

  $$(C_1, C_2) \text{ is a maximal CSS-T pair } \Leftrightarrow C_1^{\perp} = C_1 \star C_2 \text{ and } C_2^{\perp} = C_1^{\star 2}.$$

  Moreover, we determine minimal (Corollary G.3.3) and maximal (Proposition G.3.5 and Corollary G.3.10) elements of the poset $\mathcal{P}$: (C_1, C_2) is a maximal CSS-T pair

  - with respect to C_2 if and only if

    $$C_2 = C_1 \cap (C_1^{\star 2})^{\perp}.$$

  - with respect to C_1 if and only if

    $$C_1 = C_2^{\perp} \cap (C_1 \star C_2)^{\perp}.$$

- Corollary G.3.9 contains a propagation rule for nondegenerate CSS-T codes: Given a nondegenerate $[[n, k, d]]$ CSS-T code from a CSS-T pair (C_1, C_2), for any $y \in C_2^{\perp} \cap (C_1 \star C_2)^{\perp}$ and $y \notin C_1$, we have that $(C_1 + \langle y \rangle, C_2)$ is a nondegenerate CSS-T pair with parameters $[[n, k+1, d]]$.

- In Theorem G.4.8, we prove that for cyclotomic cosets $I_1, I_2 \subset \mathbb{Z}_n$,

  $$(C(I_1), C(I_2)) \text{ is a CSS-T pair if and only if } I_2 \subset I_1 \text{ and } n \notin (I_1 + I_1 + I_2).$$

  The corresponding quantum code is a $[[n, |I_1| - |I_2|, \geq n - \mathrm{Amp}(J_2) + 1]]$ code.

G.1.2 Motivating example

We conclude this section with an example to demonstrate the utility of some of the results in the paper. In particular, we show how to apply them to the well known $[[15, 1, 3]]$ (punctured) quantum Reed-Muller code [1, 18]. Let $m \geq 1$ and $0 \leq d \leq m-1$. Then the d-th order *binary Reed-Muller code* is defined as

$$\mathrm{RM}_m(d) := \left\{ (f(v))_{v \in \mathbb{F}_2^m} : f \in \mathbb{F}_2[x_1, \ldots, x_m], \deg f \leq d \right\}.$$

Moreover, it is known that its dual code is $\mathrm{RM}_m(d)^\perp = \mathrm{RM}_m(m-1-d)$. Let $m = 4$ and assume that we order the points in $\mathbb{F}_2^4$ so that $(0,0,0,0)$ corresponds to the first coordinate of the corresponding Reed-Muller codes. We consider $C_1 = \mathrm{RM}_4(1)^{\{1\}}$, that is, the puncturing of the code $\mathrm{RM}_4(1)$ in the coordinate corresponding to $(0,0,0,0)$. For C_2, we consider the simplex code of length 15. This corresponds to taking $C_2 = \mathrm{RM}_4(1)_{\{1\}}$, the shortening of $\mathrm{RM}_4(1)$ in the first coordinate. The sets of monomials whose evaluation over $\mathbb{F}_2^4 \backslash \{(0,0,0,0)\}$ generates C_1 and C_2 are $\{1, x_1, x_2, x_3, x_4\}$ and $\{x_1, x_2, x_3, x_4\}$, respectively, and we have $C_2 \subset C_1$. If we prove that $C_2 \subset (C_1^{\star 2})^\perp$, then $C_2 \subset C_1 \cap (C_1^{\star 2})^\perp$, and, by Theorem G.2.3, we would have that (C_1, C_2) is a CSS-T pair. The Schur product $\mathrm{RM}_m(d_1) \star \mathrm{RM}_m(d_2)$, for some $0 \leq d_1, d_2 \leq m-1$, corresponds to taking the code generated by the evaluation of the products of the corresponding monomials. In this example, $C_1^{\star 2} = C_1 \star C_1$ is the code generated by the evaluation over $\mathbb{F}_2^4 \setminus \{(0,0,0,0)\}$ of

$$\{1, x_1, x_2, x_3, x_4, x_1x_2, x_1x_3, x_1x_4, x_2x_3, x_2x_4, x_3x_4\}.$$

This actually corresponds to the puncturing in the first position of $\mathrm{RM}_4(2)$, that is, $C_1^{\star 2} = \mathrm{RM}_4(2)^{\{1\}}$. Since the dual of a puncturing is the corresponding shortening of the dual, we obtain $(C_1^{\star 2})^\perp = \mathrm{RM}_4(1)_{\{1\}} = C_2$. Thus, (C_1, C_2) is a CSS-T pair. Analogously, one can prove that $C_1 \star C_2$ is generated by

$$\{x_1, x_2, x_3, x_4, x_1x_2, x_1x_3, x_1x_4, x_2x_3, x_2x_4, x_3x_4\},$$

that is, $C_1 \star C_2 = \mathrm{RM}_4(2)_{\{1\}} = C_1^\perp$. We proved before that $(C_1^{\star 2})^\perp = C_2$, which implies $C_1^{\star 2} = C_2^\perp$. By Theorem G.3.11, we have that the $[[15, 1, 3]]$ (punctured) quantum Reed-Muller code is maximal with respect to the CSS-T poset $\mathcal{P}$.

G.2 Equivalent Definitions

In this section, we give equivalent conditions for a pair of binary codes (C_1, C_2) to be a CSS-T pair.

We start by fixing some notations for the rest of the paper. For a positive integer n, we write $[n] := \{1, \ldots, n\}$. We denote by $\mathbb{1}$ the element $(1, \ldots, 1)$, where the number of entries depends on the context. We say a binary code C of length n, dimension k, and minimum Hamming distance d is an $[n, k, d]$ code. Let $C \subset \mathbb{F}_2^n$ be a code and $i \in [n]$. The *dual* of C with respect to the Euclidean inner product is denoted by $C^\perp$. The *shortening* of C in $\{i\}$, denoted by $C_{\{i\}}$, is the binary code

$$C_{\{i\}} := \{(c_1, \ldots, c_{i-1}, c_{i+1}, \ldots, c_n) : (c_1, \ldots, c_{i-1}, 0, c_{i+1}, \ldots, n) \in C\}.$$

The *puncturing* of C in $\{i\}$, denoted by $C^{\{i\}}$, is the binary code

$$C^{\{i\}} := \{(c_1, \ldots, c_{i-1}, c_{i+1}, \ldots, c_n) : (c_1, \ldots, c_{i-1}, c_i, c_{i+1}, \ldots, c_n) \in C, \text{for some } c_i \in \mathbb{F}_2\}.$$

For $S \subset [n]$, we write C_S (resp. C^S) for the successive shortening (resp. puncturing) of C in the coordinates indexed by the elements in S.

The *Schur product* of two vectors $x = (x_1, \ldots, x_n)$ and $y = (y_1, \ldots, y_n)$ in $\mathbb{F}_2^n$ is denoted and defined by

$$x \star y := (x_1 y_1, \ldots, x_n y_n).$$

The *Schur product* of two binary codes C_1 and C_2, denoted by $C_1 \star C_2$, is defined as the binary code generated by the vectors

$$\{c_1 \star c_2 : c_i \in C_i\}.$$

The *t-fold Schur product* of C with itself is $C^{\star t} := \underbrace{C \star \cdots \star C}_{t}$, the t-th Schur power of C. Note that for a binary code C, we always have $C \subset C^{\star 2}$ since $x \star x = x$ for any binary vector $x \in \mathbb{F}_2^n$.

Recall that a code is *of even weight*, or *even-weighted*, provided all of its codewords have even Hamming weight. For $x \in C$, we use $Z(x)$ to denote the set of positions of the zero coordinates of x, i.e., $Z(x) = [n] \setminus \mathrm{supp}(x)$, where $\mathrm{supp}(x)$ is the support of x (set of nonzero entries of x).

We use $[[n, k, d]]$ to denote a quantum code that encodes k logical qubits into n physical qubits and can correct up to $d - 1$ erasures. We recall the CSS construction [8, 23].

Theorem G.2.1 CSS Construction**.** Let $C_i \subset \mathbb{F}_2^n$ be linear codes of dimension k_i, for $i = 1, 2$, such that $C_2 \subset C_1$. Then, there is an $[[n, k_1 - k_2, d]]$ quantum code with

$$d = \min\left\{\mathrm{wt}\left(C_1 \setminus C_2\right), \mathrm{wt}\left(C_2^{\perp} \setminus C_1^{\perp}\right)\right\}.$$

Let $d^* := \min\{\mathrm{wt}(C_1), \mathrm{wt}(C_2^{\perp})\}$. If $d = d^*$, the corresponding quantum code is said to be *nondegenerate*, and it is called *degenerate* if $d > d^*$.

The following definition was given in [20].

Definition G.2.2. Let $C_2 \subset C_1$ be binary codes. Then (C_1, C_2) is a *CSS-T pair* if C_2 is even-weighted and for any $x \in C_2$, the shortening $(C_1^{\perp})_{Z(x)}$ contains a self-dual code.

Theorem G.2.3. Let C_1 and C_2 be binary codes of length n. The following are equivalent.

(1) (C_1, C_2) is a CSS-T pair.

(2) $C_2 \subset C_1$, C_2 is even-weighted, and for any $x \in C_2$ the code $C_1^{Z(x)}$ is self-orthogonal.

(3) $C_2 \subset C_1 \cap (C_1^{\star 2})^{\perp}$.

(4) $C_1^{\perp} + C_1^{\star 2} \subset C_2^{\perp}$.

Moreover, if (C_1, C_2) is a CSS-T pair then C_2 is self-orthogonal.

Proof. The equivalence of (1) and (2) was proved in [2]. (See also [4] for the case of arbitrary fields of characteristic 2.) Also, (3) and (4) are equivalent by taking the duals.

To show the equivalence of (2) and (3), note that for any $x \in C_2$, the code $C_1^{Z(x)}$ is self-orthogonal if and only if $x \in (C_1^{\star 2})^{\perp}$. Indeed, $x \in (C_1^{\star 2})^{\perp}$ if and only if $\sum_{i=1}^{n} x_i u_i v_i = 0$ for any $u, v \in C_1$. As x is a binary vector, we can write this as $\sum_{i \in \mathrm{supp}(x)} u_i v_i = 0$, i.e., $u' \cdot v' = 0$ for any $u', v' \in C_1^{Z(x)}$, that is $C_1^{Z(x)}$ is self-orthogonal. On the other hand, if $C_2 \subset C_1 \cap (C_1^{\star 2})^{\perp}$, then we have

$$C_2 \subset C_1 \subset C_1^{\star 2} \subset C_2^{\perp}.$$

Thus, C_2 is even-weighted because it is self-orthogonal. □

Remark G.2.4. Note that if (C_1, C_2) is a CSS-T pair then, by part (4) of Theorem G.2.3, $C_1^{\star 2} \subset C_2^{\perp}$, which is equivalent to $C_1 \star C_2 \subset C_1^{\perp}$. This observation previously appeared in [20, Remark 3].

A *CSS-T code* is a code obtained via a CSS-T pair and Theorem G.2.1. The equivalences of Theorem G.2.3 allow us to see some structural properties of CSS-T codes. In particular, the minimum distance of a CSS-T code associated with (C_1, C_2) is lower bounded by the minimum distance of $C_2^{\perp}$.

Corollary G.2.5. Let (C_1, C_2) be a CSS-T pair. Then

$$\min\{\mathrm{wt}(C_1), \mathrm{wt}(C_2^{\perp})\} = \mathrm{wt}(C_2^{\perp}),$$

and the parameters of the corresponding CSS-T code are

$$[[n, k_1 - k_2, \geq \mathrm{wt}(C_2^{\perp})]].$$

Moreover, if the code is nondegenerate, we have equality in the minimum distance.

Proof. From Theorem G.2.3 (4), we see that

$$\mathrm{wt}(C_2^{\perp}) \leq \mathrm{wt}(C_1^{\perp} + C_1^{\star 2}) \leq \mathrm{wt}(C_1^{\star 2}) \leq \mathrm{wt}(C_1).$$

□

G.3 The poset of CSS-T pairs

Let (C_1, C_2) be a CSS-T pair. By Corollary G.2.5, the CSS-T code associated with the pair (C_1, C_2) has parameters $[[n, k_1 - k_2, \geq \mathrm{wt}(C_2^{\perp})]]$. Thus, increasing the dimension of C_1 will increase the dimension of the associated CSS-T code, and the minimum distance is still bounded by $\mathrm{wt}(C_2^{\perp})$. In particular, if the associated CSS-T code is nondegenerate, then increasing the dimension of C_1 does not change the minimum distance (see Corollary G.2.5). On the other hand, increasing the dimension of C_2 could improve the minimum distance but decrease the dimension of the resulting CSS-T code.

The following Corollary allows us to define a partial order on the set of CSS-T pairs. The result shows that all the CSS-T pairs are determined by those CSS-T pairs (C_1, C_2) that cannot be extended to another CSS-T pair (C_1', C_2'), where $C_1 = C_1'$ or $C_2 = C_2'$.

Corollary G.3.1. Let (C_1, C_2) be a CSS-T pair. Then, the following hold.

(1) (C_1', C_2) is a CSS-T pair for any $C_2 \subset C_1' \subset C_1$.

(2) (C_1, C_2') is a CSS-T pair for any $C_2' \subset C_2$.

Proof. (1) As $C_1' \subset C_1$, then $(C_1'^{\perp})_{Z(x)} \supset (C_1^{\perp})_{Z(x)}$ for any $x \in C_2$. Hence, if $(C_1^{\perp})_{Z(x)}$ contains a self-dual code, then $(C_1'^{\perp})_{Z(x)}$ also contains a self-dual code.
(2) It is a direct consequence of Theorem G.2.3 (2). □

We are ready to define a partial order in the set of CSS-T pairs.

Definition G.3.2. We denote by $\mathcal{P}$ the *poset* of CSS-T pairs relative to the order $(C_1, C_2) \leq (C_1', C_2')$ if and only if $C_i \subset C_i'$ for $i = 1, 2$.

From now on, we discard the trivial pairs $(C_1, \{0\})$ from $\mathcal{P}$. Denote by $\langle x \rangle$ the code generated by an element $x \in \mathbb{F}_2^n$.

Corollary G.3.3. The set of minimal elements of $\mathcal{P}$ is

$$\{(\langle u \rangle, \langle u \rangle) : u \text{ even }, u \in \mathbb{F}_2^n\}.$$

Proof. This is a consequence of Corollary G.3.1. □

We are interested in the set of maximal elements of $\mathcal{P}$.

Definition G.3.4. We say that $(C_1, C_2) \in \mathcal{P}$ is *maximal in* C_1 if $(C_1, C_2) \leq (C_1', C_2)$ implies $C_1 = C_1'$. Similarly, (C_1, C_2) is *maximal in* C_2 if $(C_1, C_2) \leq (C_1, C_2')$ implies $C_2 = C_2'$.

Note that a pair (C_1, C_2) is a maximal element of $\mathcal{P}$ if and only if (C_1, C_2) is maximal in both C_1 and C_2. Some maximal elements in $\mathcal{P}$ are given by the pairs (C_1, C_2) where C_1 has codimension one. Indeed, by Theorem G.2.3 (4), $C_1^{\star 2} \subset C_2^{\perp}$. Since we assume that C_2 is nontrivial, we see that $C_1^{\star 2}$ is a proper subspace of $\mathbb{F}_2^n$, obtaining thus that $C_1 = C_1^{\star 2} = C_2^{\perp}$. Hence, C_2 is a one-dimensional subspace of C_1 generated by an even-weight vector. In fact, we show in Theorem G.3.11 that the property $C_1^{\star 2} = C_2^{\perp}$ holds for any maximal pair (C_1, C_2).

We start by describing pairs that are maximal in C_2.

Proposition G.3.5. A pair $(C_1, C_2) \in \mathcal{P}$ is maximal in C_2 if and only if $C_2 = C_1 \cap (C_1^{\star 2})^{\perp}$.

Proof. This is provided by Theorem G.2.3 (3). □

The following proposition gives a criterion for extending a CSS-T pair (C_1, C_2) to a pair (C_1', C_2) with $\dim C_1' = \dim C_1 + 1$.

Proposition G.3.6. Let (C_1, C_2) be a CSS-T pair and $y \in \mathbb{F}_2^n$. Then $(C_1 + \langle y \rangle, C_2)$ is a CSS-T pair if and only if $C_1 \star y + \langle y \rangle \subset C_2^{\perp}$, or equivalently, $y \in C_2^{\perp} \cap (C_1 \star C_2)^{\perp}$.

Proof. Define $C_1' := C_1 + \langle y \rangle$. Note that $C_1'^{\perp} \subset C_1^{\perp}$. Since (C_1, C_2) is a CSS-T pair, we have $C_1^{\perp} + C_1^{\star 2} \subset C_2^{\perp}$ by Theorem G.2.3 (4). Thus,

$$C_1'^{\perp} \subset C_1^{\perp} \subset C_1^{\perp} + C_1^{\star 2} \subset C_2^{\perp}.$$

By Theorem G.2.3 (4), (C_1', C_2) is a CSS-T pair if and only if $C_1'^{\perp} + C_1'^{\star 2} \subset C_2^{\perp}$. So, it is enough to verify $C_1'^{\star 2} \subset C_2^{\perp}$ if and only if $C_1 \star y + \langle y \rangle \subset C_2^{\perp}$. It remains to notice that $C_1'^{\star 2} = C_1^{\star 2} + C_1 \star y + \langle y \rangle$, as $y \star y = y$. □

Unlike Proposition G.3.5, Proposition G.3.6 does not allow us to find the maximal C_1 for a given C_2 to get a CSS-T pair as the next example shows.

Example G.3.7. Let $C = \langle (1,1,1,1,1,1) \rangle$. By Proposition G.3.3, $(C, C) \in \mathcal{P}$ and it is a minimal element. We have $C^{\perp} \cap (C^{\star 2})^{\perp} = C^{\perp}$. Let $v = (1,1,1,1,0,0), w = (1,0,0,0,0,1) \in C^{\perp}$. Thus $(C + \langle v \rangle, C) \in \mathcal{P}$, but $(C + \langle v, w \rangle, C) \notin \mathcal{P}$, despite $v, w \in C^{\perp}$.
We have:

$$C^{\perp} \cap ((C + \langle v \rangle) \star C)^{\perp} = \langle (1,1,0,0,0,0), (1,0,1,0,0,0), (1,0,0,1,0,0), (0,0,0,0,1,1) \rangle.$$

We can take any non-zero element v' different from $(1,1,1,1,1,1,1)$ in this intersection and we get that $(C + \langle v, v' \rangle, C)$ is a CSS-T pair. Note that for v' equal to $(1,1,0,0,0,0)$, $(1,0,1,0,0,0)$, or $(1,0,0,1,0,0)$, we get a new CSS-T pair. However, we do not obtain a new CSS-T for $v' = (0,0,0,0,1,1)$ since $v' \in C + \langle v \rangle$.

Remark G.3.8. Note that, if (C_1, C_2) is a CSS-T pair, then so is $(C_1 + \langle \mathbb{1} \rangle, C_2)$. This follows from Theorem G.2.3 (3), the previous result, and the observation that $C_2 \subset \langle \mathbb{1} \rangle^{\perp}$, as C_2 is even-weighted.

Proposition G.3.6 also provides the following propagation rule for nondegenerate CSS-T codes.

Corollary G.3.9. Let (C_1, C_2) be a CSS-T pair such that the associated $[[n, k, d]]$ CSS-T code is nondegenerate. For any $y \in C_2^{\perp} \cap (C_1 \star C_2)^{\perp}$ and $y \notin C_1$, the pair $(C_1 + \langle y \rangle, C_2)$ is a nondegenerate CSS-T pair with parameters

$$[[n, k+1, d]].$$

Proof. By Proposition G.3.6, $(C_1 + \langle y \rangle, C_2)$ is a CSS-T pair, and the parameters follow from Corollary G.2.5. □

Corollary G.3.10. A pair $(C_1, C_2) \in \mathcal{P}$ is maximal in C_1 if and only if $C_1 = C_2^{\perp} \cap (C_1 \star C_2)^{\perp}$.

Proof. By Proposition G.3.6, $(C_1, C_2) \in \mathcal{P}$ is maximal in C_1 if and only $C_2^{\perp} \cap (C_1 \star C_2)^{\perp} \subset C_1$. On the other hand, the pair $(C_1 + \langle y \rangle, C_2)$ is CSS-T for each $y \in C_1$, so by Proposition G.3.6, $C_1 \subset C_2^{\perp} \cap (C_1 \star C_2)^{\perp}$ as well. □

We obtain the following theorem by combining the previous results on maximality in C_1 and C_2.

Theorem G.3.11. Let $C_2 \subset C_1 \subset \mathbb{F}_2^n$ be linear codes. The pair (C_1, C_2) is maximal in $\mathcal{P}$ if and only if

(1) $C_1^\perp = C_1 \star C_2$ and

(2) $C_2^\perp = C_1^{\star 2}$.

Proof. Assume (C_1, C_2) is a maximal CSS-T pair. Note that we can assume $\mathbb{1} \in C_1$ by Remark G.3.8, and we have $C_2 = \langle \mathbb{1} \rangle \star C_2 \subset C_1 \star C_2$. Now, by Corollary G.3.10, we have

$$C_1^\perp = C_2 + C_1 \star C_2 = C_1 \star C_2,$$

which shows (1).

As $C_2 = C_1 \cap (C_1^{\star 2})^\perp$ by Proposition G.3.5, we only need to show that $(C_1^{\star 2})^\perp \subset C_1$ in order to prove (2). Since $C_2 \subset C_1$, we have $C_1 \star C_2 \subset C_1^{\star 2}$ and $(C_1^{\star 2})^\perp \subset (C_1 \star C_2)^\perp$. Also, $C_2 \subset C_1 \subset C_1^{\star 2}$ implies that $(C_1^{\star 2})^\perp \subset C_2^\perp$. Therefore, by Corollary G.3.10, we get

$$(C_1^{\star 2})^\perp \subset C_2^\perp \cap (C_1 \star C_2)^\perp = C_1.$$

Theorem G.2.3 (2) implies that (C_1, C_2) is a CSS-T pair. The maximality follows directly from Proposition G.3.5 and Corollary G.3.10, using both (1) and (2). □

The following example illustrates that the necessary condition (2) of Theorem G.3.11 for (C_1, C_2) to be maximal is not sufficient.

Example G.3.12. Define $C_2 := \langle (1,1,0,0,0,0) \rangle$ and C_1 as the code whose generator matrix is given by

$$\begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix}.$$

It is not difficult to see using [3, 15] that a generator matrix for $C_1^{\star 2}$ is given by

$$\begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Hence, $(C_1^{\star 2})^\perp = \langle (1,1,0,0,0,0) \rangle = C_2$, meaning that the pair (C_1, C_2) satisfies condition (2) of Theorem G.3.11. But the pair (C_1, C_2) is not maximal in C_1 because the extension $(C_1 + \langle \mathbb{1} \rangle, C_2)$ satisfies (1)–(2) of Theorem G.3.11, meaning that it is maximal.

In the following Corollary, we collect special cases when the conditions of Theorem G.3.11 can be relaxed.

Corollary G.3.13. Let C be a binary code.

(1) The pair (C, C) is maximal in $\mathcal{P}$ if and only if $C^{\star 2} = C^\perp$.

(2) If $C^\perp \subset C$, the pair $(C, C^\perp)$ is maximal in $\mathcal{P}$ if and only if $C^{\star 2} = C$. Equivalently, C is generated by vectors with pair-wise disjoint support.

Proof. (1) If the pair (C, C) is maximal in $\mathcal{P}$, then $C^{\star 2} = C^{\perp}$ by Theorem G.3.11 (2). If $C^{\star 2} = C^{\perp}$, then (C, C) is a CSS-T pair by Theorem G.2.3 (3). Also, the pair (C, C) is maximal in $\mathcal{P}$ by Theorem G.3.11.

(2) If $(C, C^{\perp})$ is a maximal CSS-T pair, then $C = C^{\star 2}$ by Theorem G.3.11 (2). Conversely, assume that $C = C^{\star 2}$. Theorem G.2.3 (3) verifies that $(C, C^{\perp})$ is a CSS-T pair. Proposition G.3.5 verifies that $(C, C^{\perp})$ is maximal in $C^{\perp}$. If $(C + \langle y \rangle, C^{\perp})$ is a CSS-T pair for some $y \in \mathbb{F}_2^n$, then $y \in C$ by Proposition G.3.6, meaning that $(C, C^{\perp})$ is maximal in C. □

Example G.3.14. Assume $3d = m - 1$ for some $d, m \in \mathrm{N}$. For the binary Reed-Muller code $C := \mathrm{RM}_m(d)$, we have

$$C^{\perp} = \mathrm{RM}_m(d)^{\perp} = \mathrm{RM}_m(m - d - 1) = \mathrm{RM}_m(2d) = C^{\star 2}.$$

Thus, (C, C) is a maximal pair by Corollary G.3.13 (1).

Observe that even if (C_1, C_2) is maximal in $\mathcal{P}$, in principle, there can be a pair $(D_1, D_2) \in \mathcal{P}$ such that $C_2 \subset D_2$ or $C_1 \subset D_1$. We can give a complete characterization of such spaces. First we need a lemma.

Lemma G.3.15. Let $C \subsetneq \mathbb{F}_2^n$ such that for any $x \in C \cap (C^{\star 2})^{\perp}$ we have $C \star x = C^{\perp}$. Then $(C^{\star 2})^{\perp} = \langle y \rangle$, for some $y \in C$, or $C = C^{\perp}$ and $C^{\star 2} = \langle \mathbb{1} \rangle^{\perp}$.

Proof. First observe that $C \star x = C^{\perp} \subset C^{\star 2}$ implies $(C^{\star 2})^{\perp} \subset C$ and thus $C \cap (C^{\star 2})^{\perp} = (C^{\star 2})^{\perp}$. Let $y \in (C^{\star 2})^{\perp}$ be a minimal support codeword. If $y = \mathbb{1}$, then $C \star y = C = C^{\perp}$ and $C^{\star 2} = \langle \mathbb{1} \rangle^{\perp}$.

Assume now that $\mathrm{wt}(y) < n$. Since $C \star y = C^{\perp}$ then $\langle e_i \ : \ i \notin \mathrm{supp}(y) \rangle \subseteq C$. If there is another minimal codeword $y \neq x \in (C^{\star 2})^{\perp}$, the same arguments lead to the existence of $i \in \mathrm{supp}(y) \setminus \mathrm{supp}(x)$ such that $e_i \in C^{\star 2}$ and thus $z_i = 0$ for any $z \in (C^{\star 2})^{\perp}$, which contradicts that $y_i \neq 0$. Thus, there are no more minimal codewords in $(C^{\star 2})^{\perp}$ and we have the conclusion. □

The next example shows that the converse of the last lemma is not true.

Example G.3.16. Let $C = \langle (1,1,0,0,0), (0,1,1,0,0), (0,0,0,1,1) \rangle$. We have

$$C^{\star 2} = \langle (1,0,0,0,0), (0,1,0,0,0), (0,0,1,0,0), (0,0,0,1,1) \rangle,$$

and $(C^{\star 2})^{\perp} = \langle (0,0,0,1,1) \rangle$. However,

$$C \star (0,0,0,1,1) = (0,0,0,1,1) \subsetneq C^{\perp} = \langle (1,1,1,0,0), (0,0,0,1,1) \rangle.$$

Proposition G.3.17. Let $(C_1, C_2) \in \mathcal{P}$. Then

1. There is no $(D_1, D_2) \in \mathcal{P}$ with $C_1 \subsetneq D_1$ if and only if $C_1^{\perp} = C_1 \star y$ for any $y \in C_1 \cap (C_1^{\star 2})^{\perp}$.

2. There is no $(D_1, D_2) \in \mathcal{P}$ with $C_2 \subsetneq D_2$ if and only if (C_2, C_2) is maximal.

Proof. If there is no such D_1, since for any $y \in C_1 \cap (C_1^{\star 2})^\perp$, $(C_1, \langle y \rangle) \in \mathcal{P}$ but C_1 cannot be extended, then $C_1 = \langle y \rangle^\perp \cap (C_1 \star y)^\perp = (C_1 \star y)^\perp$ by Corollary G.3.10 (note that $y \in C_1$ implies $y \in C_1 \star y$). On the other hand, assume $C_1^\perp = C_1 \star y$ for any $y \in C_1 \cap (C_1^{\star 2})^\perp$, and let $C_1 \subset D_1$ such that D_1 is the largest code containing C_1 with $(D_1, D) \in \mathcal{P}$ for some D. By the first part of this proof, the hypothesis and Lemma G.3.15 we have $(D_1^{\star 2})^\perp \subseteq (C_1^{\star 2})^\perp = \langle y \rangle$ for some $y \in C_1$. This implies $D_1 \cap (D_1^{\star 2})^\perp = \langle y \rangle$ because $(D_1, D) \in \mathcal{P}$. By the choice of D_1 and the first part of the proof, $D_1 \star y = D_1^\perp$, and we also have $C_1 \star y = C_1^\perp$. Thus,

$$C_1 \star y \subset D_1 \star y = D_1^\perp \subset C_1^\perp \Rightarrow D_1^\perp = C_1^\perp,$$

and we get $D_1 = C_1$.

To prove (2), observe that $(D_1, D_2) \in \mathcal{P}$ is such that $C_2 \subset D_2$ if and only if there is $y \notin C_2$ such that $(C_2 + \langle y \rangle, C_2) \in \mathcal{P}$ by Corollary G.3.1. This happens if and only if $y \in (C_2^\perp \cap (C_2^{\star 2})^\perp) \setminus C_2$ by Proposition G.3.6. However, $(C_2^{\star 2})^\perp \subset C_2^\perp$ and thus, $y \in (C_2^{\star 2})^\perp \setminus C_2$. If there is not such y, it means that $(C_2^{\star 2})^\perp = C_2$ and by Corollary G.3.13 we have the conclusion. □

Example G.3.18. Let

$$G = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \end{pmatrix}$$

and C be the code generated by G. We can check that $C^{\star 2} = \langle \mathbb{1} \rangle^\perp$, $C = C^\perp$ and thus, $(C, \langle \mathbb{1} \rangle) \in \mathcal{P}$ and there is no other CSS-T pair (D_1, D_2) with $C_1 \subsetneq D_1$.

Corollary G.3.19. If $(C_1, C_2) \in \mathcal{P}$ and there is no $D_1 \supsetneq C_1$ and D_2 such that $(D_1, D_2) \in \mathcal{P}$, then for some $y \in C_1$, $C_2 = \langle y \rangle$ and (C_1, C_2) is maximal.

G.4 Cyclic codes

We now illustrate the results from the previous sections using cyclic codes (and extended cyclic codes). We will review cyclic codes over $\mathbb{F}_q$, but note that we restrict to the case $q = 2$ whenever we refer to CSS-T codes.

Take an integer $s > 1$ and consider the field extension $\mathbb{F}_{q^s}/\mathbb{F}_q$. We set n with $n \mid q^s - 1$ and $g \in \mathbb{F}_q[x]$ such that g divides $x^n - 1$. We denote by C_g the cyclic code with g as its generator polynomial. Let $\beta \in \mathbb{F}_{q^s}$ be a primitive n-th root of unity. For the set $\mathbb{Z}_n := \mathbb{Z}/n\mathbb{Z}$, we will consider the representatives between 1 and n, i.e., $\mathbb{Z}_n = \{1, 2, \ldots, n\}$.

Definition G.4.1. The *defining set* is given by $J := \{j \in \mathbb{Z}_n : g(\beta^j) = 0\}$ and the *generating set* by $I := \{i \in \mathbb{Z}_n : g(\beta^i) \neq 0\}$.

Note that $J = [n] \setminus I$, and

$$g = \prod_{j \in J} (x - \beta^j) = \frac{x^n - 1}{\prod_{i \in I} (x - \beta^i)}.$$

Define $-I := \{n - i : i \in I\} \subset \mathbb{Z}_n$. Let $\mathcal{M} \subset \mathbb{Z}_{\geq 0}$ be a finite set. We consider the $\mathbb{F}_{q^s}$-linear subspace

$$\mathcal{L}(\mathcal{M}) := \langle x^i : i \in \mathcal{M} \rangle \subset \mathbb{F}_{q^s}[x].$$

Take a set of points $X = \{P_1, \ldots, P_{|X|}\} \subset \mathbb{F}_{q^s}$. We can define the following evaluation map associated to X:

$$\begin{array}{rccc} \mathrm{ev}_X : & \mathbb{F}_{q^s}[x] & \to & \mathbb{F}_{q^s}^{|X|} \\ & f & \mapsto & \big(f(P_1), \ldots, f(P_{|X|})\big). \end{array}$$

Let $X_n := \{1, \beta, \ldots, \beta^{n-1}\}$, i.e., X_n is the zero locus of $x^n - 1$ in $\mathbb{F}_{q^s}$. We now consider the associated evaluation code

$$B(\mathcal{M}) := \mathrm{ev}_{X_n}(\mathcal{L}(\mathcal{M})) = \{(f(1), f(\beta), \ldots, f(\beta^{n-1})) : f \in \mathcal{L}(\mathcal{M})\} \subset \mathbb{F}_{q^s}^n,$$

and we define

$$C(I) := B(-I) \cap \mathbb{F}_q^n.$$

From [5], we obtain that $C_g = C(I)$, i.e., we have a description of cyclic codes in terms of subfield subcodes of evaluation codes.

The definitions clearly show that J and I are closed under multiplication by q, which leads to the following definition.

Definition G.4.2. Given a subset $I \subset \mathbb{Z}_n$, denote $q \cdot I := \{q \cdot i : i \in I\}$. We say that I is a *cyclotomic coset* if $I = q \cdot I$. Let $a \in \mathbb{Z}_n$, the set $\mathfrak{I}_a := \{q^j \cdot a : j \geq 0\} \subset \mathbb{Z}_n$ is the *minimal cyclotomic coset* associated to a.

Example G.4.3. Let $q = 2$, $s = 4$, and $n = 15$. Then, the minimal cyclotomic cosets are

$$\mathfrak{I}_1 = \{1, 2, 4, 8\},\ \mathfrak{I}_3 = \{3, 6, 12, 9\},\ \mathfrak{I}_5 = \{5, 10\},\ \mathfrak{I}_7 = \{7, 14, 13, 11\},\ \mathfrak{I}_{15} = \{15\}.$$

From [5], we have the following result about the dual of a cyclic code.

Theorem G.4.4. Let $I \subset \mathbb{Z}_n$ be a cyclotomic coset. We have that

$$C(I)^\perp = C(-J).$$

This last result can be seen as a consequence of the following fact from [5]: If I is a cyclotomic coset, then

$$(B(-I) \cap \mathbb{F}_q^n)^\perp = (B(-I)^\perp) \cap \mathbb{F}_q^n. \tag{G.4.1}$$

The length of $C(I)$ is n, and its dimension is $|I|$. For the minimum distance, we need the following definition.

Definition G.4.5. The *amplitude* of a nonempty subset $I \subset \mathbb{Z}_n$ is

$$\mathrm{Amp}(I) := \min\{i \in \mathrm{N} : \exists c \in \mathbb{Z}_n \text{ such that } I \subset \{c, c+1, \ldots, c+i-1\}\}.$$

Then, the minimum distance of $C(I)$ is greater than or equal to $n - \mathrm{Amp}(I) + 1$; for example, see [10]. Summarizing, $C(I)$ has parameters

$$[n,\ |I|,\ \geq n - \mathrm{Amp}(I) + 1].$$

Since $\mathrm{Amp}(-J) = \mathrm{Amp}(J)$, we see that $C(I)^\perp$ has parameters $[n, |J|, \geq n - \mathrm{Amp}(J) + 1]$. Note that $n - \mathrm{Amp}(J) + 1$ is equal to the usual BCH bound, i.e., it is equal to $\delta(I) + 1$, where $\delta(I)$ is the maximum number of consecutive elements in I.

Given $I_1, I_2 \subset \mathbb{Z}_n$, we consider their Minkowski sum

$$I_1 + I_2 := \{i_1 + i_2 : i_1 \in I_1,\ i_2 \in I_2\} \subset \mathbb{Z}_n. \tag{G.4.2}$$

It is easy to check that if $I_1, I_2 \subset \mathbb{Z}_n$ are cyclotomic cosets, then $I_1 + I_2$ is also a cyclotomic coset. Following the previous notation, we will denote $J_i = [n] \setminus I_i$, for $i = 1, 2$.

Example G.4.6. Continuing with Example G.4.3, we consider

$$I_1 = \{1, 2, 4, 8, 15\},\ I_2 = \{1, 2, 4, 8\}.$$

We compute the following Minkowski sums, which we will use in the following examples:

$$I_1 + I_2 = \{1, 2, 3, 4, 5, 6, 8, 9, 10, 12\},\ I_1 + I_1 = (I_1 + I_2) \cup \{15\}.$$

Note that $I_1 + I_2 = \mathfrak{I}_1 \cup \mathfrak{I}_3 \cup \mathfrak{I}_5$, i.e., $I_1 + I_2$ is also a cyclotomic coset.

The following result from [11] shows that the sum and the Schur product of cyclic codes is also a cyclic code.

Lemma G.4.7. Let I_1 and I_2 be cyclotomic cosets. Then

$$C(I_1) + C(I_2) = C(I_1 \cup I_2),$$
$$C(I_1) \star C(I_2) = C(I_1 + I_2).$$

As an application of Theorem G.2.3, we obtain the following criterion for a pair of cyclic codes to be a CSS-T pair.

Theorem G.4.8. Let $I_1, I_2 \subset \mathbb{Z}_n$ be cyclotomic cosets. Then $(C(I_1), C(I_2))$ is a CSS-T pair if and only if:

(1) $I_2 \subset I_1$ and

(2) $n \notin (I_1 + I_1 + I_2)$.

The parameters of the corresponding quantum code are $[[n, |I_1| - |I_2|, \geq n - \mathrm{Amp}(J_2) + 1]]$.

Proof. We use the third equivalent condition from Theorem G.2.3 with $C_1 = C(I_1)$ and $C_2 = C(I_2)$. We have

$$C(I_2) \subset C(I_1) \iff I_2 \subset I_1,$$

and

$$\begin{aligned} C(I_2) \subset (C(I_1)^{\star 2})^\perp &\iff \mathbb{1} \in (C(I_1)^{\star 2} \star C(I_2))^\perp = C(I_1 + I_1 + I_2)^\perp \\ &\iff \mathbb{1} \in B(-(I_1 + I_1 + I_2))^\perp \iff n \notin I_1 + I_1 + I_2, \end{aligned}$$

as follows from (G.4.1) and Lemma G.4.7. Also, the last equivalence follows from [12, Prop. 1]. We use Corollary G.2.5 for the parameters of the quantum code. □

Remark G.4.9. Theorem G.4.8 also holds if we substitute condition (2) with

(2') $I_1 + I_1 \subset -J_2$.

This is because

$$C(I_2) \subset (C(I_1)^{\star 2})^{\perp} = C(I_1 + I_1)^{\perp} \iff I_1 + I_1 \subset -J_2.$$

As $I_2 \subset I_1$, from Theorem G.4.8, we obtain the necessary condition $n \notin I_2$ for $(C(I_1), C(I_2))$ to be a CSS-T pair. This happens if and only if $n \in -J_2$. Hence, if the pair I_1, I_2 satisfies the conditions from Theorem G.4.8, then the pair $I_1 \cup \{n\}, I_2$ also satisfies those conditions. This is a translation of the following fact that we have seen in the previous section: If (C_1, C_2) is a CSS-T pair, then $(C_1 + \langle \mathbb{1} \rangle, C_2)$ is also a CSS-T pair.

Example G.4.10. We consider I_1, I_2 as in Example G.4.6. Clearly $I_2 \subset I_1$. From the computation of $I_1 + I_2$ in Example G.4.6, we obtain

$$I_1 + I_1 + I_2 = [n-1] = \{1, 2, \ldots, 14\}.$$

By Theorem G.4.8, we have that $(C(I_1), C(I_2))$ is a CSS-T pair with parameters $[[15, 1, 3]]$. Note that we have recovered the (punctured) quantum Reed-Muller code mentioned in the introduction.

In Section G.3, we studied conditions for a CSS-T pair to be maximal in each component. The following result shows how we can translate those conditions to cyclic codes.

Corollary G.4.11. Let $I_1, I_2 \subset \mathbb{Z}_n$ be cyclotomic cosets such that $(C(I_1), C(I_2))$ is a CSS-T pair. Then the pair $(C(I_1), C(I_2))$ is maximal in C_1 if and only if

$$-J_1 = I_2 \cup (I_1 + I_2),$$

is maximal in C_2 if and only if

$$-J_2 = (-J_1) \cup (I_1 + I_1),$$

and is maximal if and only if

$$-J_1 = I_1 + I_2 \text{ and } -J_2 = I_1 + I_1.$$

Proof. The conditions for maximality in C_1 and C_2 follow from Corollary G.3.10 and Proposition G.3.5, respectively, taking into account Theorem G.4.4 and Lemma G.4.7. The condition for maximality follows similarly from Theorem G.3.11. □

Example G.4.12. Continuing with the setting from Example G.4.10, it is easy to check, using Example G.4.6, that $-J_1 = I_1 + I_2$ and $-J_2 = I_1 + I_1$. Therefore, by Corollary G.4.11, the CSS-T pair $(C(I_1), C(I_2))$ is maximal.

From Corollary G.2.5, we see that it is desirable to find CSS-T pairs (C_1, C_2) such that $C_1^{\star 2}$ has a large minimum distance. In [10], it is shown that the construction of cyclic codes based on the notion of restricted weight can give rise to codes C such that both C and $C^{\star 2}$ have excellent parameters. It is, therefore, interesting to study when we can use these codes for constructing CSS-T pairs. We briefly explain the construction from [10] and then obtain CSS-T codes from this construction. In what follows, we assume that $n = q^s - 1$.

Definition G.4.13. Let $a \in [n]$ have q-ary representation $(a_{s-1}, a_{s-2}, \ldots, a_0)_q$, and let $1 \leq t \leq s$. The t-restricted weight of a is defined as

$$w_q^{(t)}(a) := \max_{i \in \{0,\ldots,s-1\}} \sum_{j=0}^{t-1} a_{i+j},$$

where we consider the sum $i + j$ modulo s. In other words, it is the maximum number of nonzero elements for any sequence of t (cyclically) consecutive digits of the q-ary representation of a.

The t-restricted weight is invariant under multiplication by q, and we can speak about the t-restricted weight of a minimal cyclotomic coset. It is shown in [10, Prop. 11] that

$$w_q^{(t)}(a) \leq w_q^{(t)}(b) + w_q^{(t)}(c),$$

for $b, c \in [n]$ and $a = b + c \bmod n$. Therefore, given cyclotomic cosets $I_1, I_2 \subset \mathbb{Z}_n$ whose elements have t-restricted weight at most μ_1, μ_2, respectively, the cyclotomic coset $I_1 + I_2$ will have t-restricted weight at most $\mu_1 + \mu_2$. Let $I^t_{\leq \mu} := \{a \in \mathbb{Z}_n : w_q^{(t)}(a) \leq \mu\}$. In [10, Prop. 13], it is proven that for $a \in I^t_{\leq \mu}$, we have $w_q^{(s)}(a) \leq \lfloor (\mu s)/t \rfloor$. This motivates the following construction.

Corollary G.4.14. Take $1 \leq t \leq s$ and $1 \leq \mu_1, \mu_2 \leq t$. If $\mu_2 \leq \mu_1$ and $2\lfloor (\mu_1 s)/t \rfloor + \lfloor (\mu_2 s)/t \rfloor \leq s - 1$, then $(C(I^t_{\leq \mu_1}), C(I^t_{\leq \mu_2}))$ is a CSS-T pair.

Proof. We use Theorem G.4.8 with $I_i = I^t_{\leq \mu_i}$, for $i = 1, 2$. As $\mu_2 \leq \mu_1$, we have $I_2 \subset I_1$. We claim that $n \notin I_1 + I_1 + I_2$. Indeed, let $z = a + b + c \bmod n$, with $a, b \in I_1$, $c \in I_2$. By the previous discussion,

$$w_2^{(s)}(z) = w_2^{(s)}(a + b + c) \leq w_2^{(s)}(a) + w_2^{(s)}(b) + w_2^{(s)}(c) \leq 2\lfloor (\mu_1 s)/t \rfloor + \lfloor (\mu_2 s)/t \rfloor \leq s - 1.$$

Since $w_2^{(s)}(n) = s$, we conclude that $n \notin I_1 + I_1 + I_2$, and the result follows from Theorem G.4.8. □

Note that, by Remark G.4.9, we can also consider $C_1 = C(I^t_{\leq \mu_1} \cup \{n\})$ for the previous result. For the parameters of the corresponding CSS-T code, in [10], there are formulas for the parameters of $C(I^t_{\leq \mu})$ in some cases, and we can also use the usual bounds for cyclic codes.

Example G.4.15. It is easy to check that I_1 and I_2 from Example G.4.6 are precisely

$$I_1 = I^4_{\leq \mu_1} \cup \{15\} \qquad \text{and} \qquad I_2 = I^4_{\leq \mu_2}$$

with $\mu_1 = \mu_2 = 1$. Note that, for $t = s = 4$, the conditions from Corollary G.4.14 are satisfied. Therefore, $(C(I^4_{\leq \mu_1}), C(I^4_{\leq \mu_2}))$ is a CSS-T pair, which implies that $(C(I_1), C(I_2))$ is a CSS-T pair (which we already knew by Example G.4.10).

G.4.1 Extended cyclic codes

We define $\hat{\mathbb{Z}}_n := \{0\} \cup \mathbb{Z}_n$. We will adapt the definitions from the previous section for this setting. Let $I \subset \hat{\mathbb{Z}}_n$. We say that I is a cyclotomic coset if $I = q \cdot I$. For $I_1, I_2 \subset \hat{\mathbb{Z}}_n$, we define $I_1 + I_2$ as in (G.4.2), where we understand that $i_1 + i_2 = 0$ if and only if $i_1 = i_2 = 0$, for $i_1 \in I_1$ and $i_2 \in I_2$, and the rest of the sums are computed as usual in $\mathbb{Z}_n = \{1, \dots, n\}$. We denote by $J := \hat{\mathbb{Z}}_n \setminus I$.

For $\mathcal{M} \subset \{0, \dots, n\}$, we consider $\hat{X}_n := \{0\} \cup X_n$, the zero locus of $x^{n+1} - x$, and we define

$$\hat{B}(\mathcal{M}) := \mathrm{ev}_{\hat{X}_n}(\mathcal{L}(\mathcal{M})) = \{(f(0), f(1), f(\beta), \dots, f(\beta^{n-1})) : f \in \mathcal{L}(\mathcal{M})\} \subset \mathbb{F}_{q^s}^{n+1}.$$

For $I \subset \hat{\mathbb{Z}}_n$ a cyclotomic coset, the extended cyclic code associated with I is

$$\hat{C}(I) := \hat{B}(I) \cap \mathbb{F}_q^{n+1}.$$

Note that in this case, we are not considering $-I$. With respect to the parameters, $\hat{C}(I)$ has parameters $[n+1, |I|, \geq n - \max(I) + 1]$, and $\hat{C}(I)^\perp$ has parameters $[n+1, n+1-|I|, \geq \delta(I) + 1]$, where $\delta(I)$ is the maximum number of consecutive elements in I as before (it is a BCH-type bound for extended cyclic codes).

Although these codes are no longer cyclic, they still preserve some of the properties of cyclic codes. The proof of the following result is analogous to the one in [10, Thm. 1].

Lemma G.4.16. Let $I_1, I_2 \subset \hat{\mathbb{Z}}_n$ be cyclotomic cosets. Then

$$\hat{C}(I_1) \star \hat{C}(I_2) = \hat{C}(I_1 + I_2).$$

As a consequence, one can check that Theorem G.4.8 and Corollary G.4.14 also hold when we consider extended cyclic codes. Moreover, for extended cyclic codes, one may also allow $\mu_1 = 0$ or $\mu_2 = 0$ in Corollary G.4.14. When considering the s-restricted weight, in [10, Prop. 10], it is shown that Corollary G.4.14 for extended cyclic codes corresponds to the family of CSS-T pairs obtained by using binary Reed-Muller codes from [2]. Nevertheless, by considering the t-restricted weight, with $t < s$, we obtain different families of CSS-T codes. Moreover, considering the general case from Theorem G.4.8, it is clear that we obtain a much larger family of CSS-T pairs than by using binary Reed-Muller codes, thus obtaining a wider range of parameters. In the following example, we show that we can improve the parameters of the CSS-T codes obtained with binary Reed-Muller codes in some cases. All the computations from the following examples were done using SageMath [24].

Example G.4.17. We use a greedy construction to obtain CSS-T codes with cyclic codes, and we compare them with the CSS-T codes obtained with binary Reed-Muller codes. Let $s > 1$, $n = 2^s - 1$, and we consider the cyclotomic cosets associated with the extension $\mathbb{F}_{2^s}/\mathbb{F}_2$. Assume that $\mathbb{Z}_n = \mathfrak{I}_{a_1} \cup \mathfrak{I}_{a_2} \cup \cdots \cup \mathfrak{I}_{a_\ell}$, with $1 = a_1 < a_2 < \cdots a_\ell$. We consider the following greedy construction: let $I_2 := \mathfrak{I}_{a_1} \cup \mathfrak{I}_{a_2} \cup \cdots \cup \mathfrak{I}_{a_t}$, for some $t < \ell$ such that $n \notin I_2 + I_2 + I_2$, and let $I_1^{(0)} := I_2$. If $I_1' := I_1^{(0)} \cup \mathfrak{I}_{a_{t+1}}$ satisfies $n \notin I_1' + I_1' + I_2$, we set $I_1^{(1)} := I_1'$, and we set $I_1^{(1)} := I_1^{(0)}$ otherwise. Following this procedure until we cannot add any more minimal cyclotomic cosets, we will get a cyclotomic coset $I_1^{(u)}$, for some

$t \leq u < \ell$, such that $n \notin I_1^{(u)} + I_1^{(u)} + I_2$. Therefore, by Theorem G.4.8 and Remark G.4.9, we get that $(C(I_1^{(u)} \cup \{n\}), C(I_2))$ is a CSS-T pair. Moreover, we have the BCH bound

$$\mathrm{wt}(C(I_2)^{\perp}) \geq n - \mathrm{Amp}(J_2) + 1 = \delta(I_2) + 1 = a_{t+1},$$

which bounds the minimum distance of the corresponding quantum code by Corollary G.2.5. Note that this construction can be easily generalized to extended cyclic codes.

For $s \leq 6$, the CSS-T codes obtained with the previous construction do not improve the parameters of the CSS-T codes obtained with binary Reed-Muller codes. Nevertheless, for $s = 7, 8, 9, 10$, we show in Table G.1 that we can obtain a broader range of parameters using cyclic and extended cyclic codes, and some of these codes outperform the ones derived from binary Reed-Muller codes. For all the codes in Tables G.1 and G.2 we have checked that the bound for the minimum distance is sharp.

Table G.1: Parameters of the CSS-T codes obtained with binary Reed-Muller, cyclic, and extended cyclic codes (using the greedy construction).

s	Reed-Muller
7	$[[128, 21, 4]]$
8	$[[256, 84, 4]]$
9	$[[512, 120, 4]]$
9	$[[512, 84, 8]]$
10	$[[1024, 375, 4]]$
10	$[[1024, 120, 8]]$

s	Cyclic	s	Extended cyclic
7	$[[127, 29, 3]]$	7	$[[128, 28, 4]]$
7	$[[127, 15, 5]]$	7	$[[128, 14, 6]]$
7	$[[127, 8, 7]]$	7	$[[128, 7, 8]]$
8	$[[255, 85, 3]]$	8	$[[256, 84, 4]]$
8	$[[255, 39, 5]]$	8	$[[256, 36, 6]]$
8	$[[255, 21, 7]]$	8	$[[256, 20, 8]]$
9	$[[511, 148, 3]]$	9	$[[512, 147, 4]]$
9	$[[511, 112, 5]]$	9	$[[512, 111, 6]]$
9	$[[511, 103, 7]]$	9	$[[512, 102, 8]]$
10	$[[1023, 376, 3]]$	10	$[[1024, 375, 4]]$
10	$[[1023, 213, 5]]$	10	$[[1024, 210, 6]]$
10	$[[1023, 191, 7]]$	10	$[[1024, 190, 8]]$
10	$[[1023, 161, 9]]$	10	$[[1024, 160, 10]]$
10	$[[1023, 131, 11]]$	10	$[[1024, 130, 12]]$
10	$[[1023, 116, 13]]$	10	$[[1024, 115, 14]]$
10	$[[1023, 106, 15]]$	10	$[[1024, 105, 16]]$

Using Remark 3.13 from [4], it is easy to see that, for n even, if we consider e_i, $1 \leq i \leq n$, the standard basis vectors in $\mathbb{F}_2^n$, and the code

$$C = \langle e_{2i-1} + e_{2i},\ 1 \leq i \leq n/2 \rangle,$$

then $(C, \langle \mathbb{1} \rangle)$ is a CSS-T pair with parameters

$$[[n, n/2 - 1, 2]]. \tag{G.4.3}$$

This code has better parameters than the CSS-T codes with minimum distance 2 derived from binary Reed-Muller, cyclic, or extended cyclic codes in the cases we have checked. Therefore, we have omitted the codes with minimum distance 2 from Table G.1 and the ones with dimension 0.

For a direct comparison, we can see that the CSS-T codes obtained from binary Reed-Muller codes with parameters $[[128, 21, 4]]$, $[[512, 120, 4]]$, $[[512, 84, 8]]$ and $[[1024, 120, 8]]$ are outperformed by the CSS-T codes derived from extended cyclic codes with parameters $[[128, 28, 4]]$, $[[512, 147, 4]]$, $[[512, 102, 8]]$ and $[[1024, 190, 8]]$, respectively.

Example G.4.18. Not all the codes from the previous example are maximal with respect to C_1. Therefore, it is possible to use our Corollary G.3.9 to increase the dimension of the corresponding quantum code in some cases. For example, one can check that the CSS-T code with parameters $[[255, 21, 7]]$ from Table G.1 is not maximal with respect to the first component using Corollary G.3.10. By Proposition G.3.6, this means that there is some vector $y \in C_2^{\perp} \cap (C_1 \star C_2)^{\perp}$ such that $y \notin C_1$ and $(C_1 + \langle y \rangle, C_2)$ is a CSS-T pair. The parameters of the corresponding quantum code are $[[255, 22, 7]]$ by Corollary G.3.9, increasing the dimension of the quantum code by 1. By computer search, we have found a vector y such that $(C_1 + \langle y \rangle, C_2)$ is still not maximal with respect to the first component. Hence, there is a vector y' such that $(C_1 + \langle y, y' \rangle, C_2)$ is a CSS-T pair with parameters $[[255, 23, 7]]$, increasing the dimension of the original quantum code by 2. In the cases where we have found such y, y', the pair $(C_1 + \langle y, y' \rangle, C_2)$ is maximal with respect to the first component, and we cannot continue to increase the dimension using Corollary G.3.9.

In Table G.2, we show the codes that can be derived from CSS-T codes using binary Reed-Muller codes, cyclic codes, and extended cyclic codes (with the greedy construction from Example G.4.17) by applying Corollary G.3.9 for length 2^s, $s = 4, \ldots, 10$ ($2^s - 1$ for cyclic codes). All the codes in Table G.2 are maximal with respect to the first component of the CSS-T pair, although it might be possible to improve them further since there are many choices for the vectors that we add to C_1 in Corollary G.3.9. We note that the CSS-T codes derived from cyclic and extended cyclic codes still outperform the improved CSS-T codes arising from Reed-Muller codes. The parity check matrices of the classical codes used to construct the quantum codes from Tables G.1 and G.2 can be found in the GitHub repository `RodrigoSanJose/Cyclic-CSS-T` [9].

Table G.2: Parameters of improved CSS-T codes obtained with binary Reed-Muller, cyclic, and extended cyclic codes (using the greedy construction).

s	Reed-Muller
5	$[[32, 4, 4]]$
7	$[[128, 26, 4]]$
9	$[[512, 133, 4]]$
10	$[[1024, 125, 8]]$

s	Cyclic
5	$[[31, 4, 3]]$
8	$[[255, 23, 7]]$
9	$[[511, 149, 3]]$
10	$[[1023, 219, 5]]$
10	$[[1023, 193, 7]]$
10	$[[1023, 133, 11]]$

s	Extended cyclic
5	$[[32, 4, 4]]$
8	$[[256, 22, 8]]$
9	$[[512, 148, 4]]$
10	$[[1024, 217, 6]]$
10	$[[1024, 192, 8]]$
10	$[[1024, 133, 12]]$

G.5 Relation to triorthogonal codes

Another family of codes that is usually studied for fault-tolerant computation, and, in particular, for magic state distillation, are triorthogonal codes [6, 17]. A binary matrix G of size $m \times n$ is called *triorthogonal* if $\mathrm{wt}(G_a \star G_b) = 0 \bmod 2$, for all pairs of rows $1 \leq a < b \leq m$, and $\mathrm{wt}(G_a \star G_b \star G_c) = 0 \bmod 2$, for all triples of rows $1 \leq a < b < c \leq m$.

With such a matrix, by taking C_1 to be the linear span of G and C_2 the linear span of the even weighted rows of G, one can construct a quantum code (which we will call *triorthogonal code*) such that, when a transversal T gate is applied to it, it induces a transversal T gate on the logical qubits, up to Clifford corrections. This is stronger than having a CSS-T code, since the definition of CSS-T only requires the physical transversal T to induce some logical operation on the logical qubits. If one wants to avoid the Clifford corrections, some weight conditions have to be imposed on the classical codes used (see [21, Thm. 4]). From our results, we can obtain the following.

Corollary G.5.1. If (C_1, C_2) is a CSS-T pair, then $\mathbb{1} \in (C_2^{\star 3})^{\perp}$.

Proof. As $C_2 \subseteq C_1$, Corollary G.3.1 implies that (C_2, C_2) is a CSS-T pair. Thus, $C_2^{\star 2} \subset C_2^{\perp}$ by Theorem G.2.3, meaning that $\mathbb{1} \in (C_2^{\star 3})^{\perp}$. □

Having $\mathbb{1} \in (C_2^{\star 3})^{\perp}$ implies that C_2 has a triorthogonal generator matrix, which is also the case for triorthogonal codes due to the fact that, in that setting, the generator matrix for C_2 is a submatrix of a triorthogonal matrix.

Since the triorthogonality condition is stronger than being CSS-T, it may be possible that CSS-T codes achieve better parameters than triorthogonal codes. To see this, we consider the *scaling exponent* of the distillation protocol presented in [6]. They obtain that

$$\gamma = \frac{\log_2(n/k)}{\log_2(d)},$$

for an $[[n, k, d]]$ triorthogonal code. Since the distillation overhead scales as $O(\log^{\gamma}(1/\epsilon))$, where ϵ is the output accuracy (see [6] for details), codes with lower γ are preferred. We will use this value for CSS-T codes to compare the goodness of their parameters with some of the triorthogonal codes in the literature. In [6], the authors find a family of triorthogonal codes with parameters $[[3k + 8, k, \geq 2]]$, where k is even. The CSS-T codes from (G.4.3) have strictly better parameters. In particular, the scaling exponent γ tends to 1 for the codes in (G.4.3), while the family from [6] has scaling exponent tending to $\log_2(3) \approx 1.585$. In [6] they also obtain a code with parameters $[[49, 1, 5]]$, and $\gamma = 2.418$. If we compare with the codes in our tables, in particular, the codes $[[32, 4, 4]]$ and $[[1024, 192, 8]]$ (to take an example of a short code and a long code), we obtain for γ the values 1.5 and 0.805, respectively.

In [17], the authors find triorthogonal codes with parameters $[[35, 3, 3]]$ and $[28, 2, 3]]$, with scaling exponent equal to 2.236 and 2.402, respectively, which are higher values than the one we obtained for $[[32, 4, 4]]$. Moreover, the authors in [17] prove that there is no triorthogonal quantum code with minimum distance larger than 3 when $n + k \leq 38$, while $[[32, 4, 4]]$ satisfies these last two conditions (but it is not triorthogonal, only CSS-T). Furthermore, in [16], triorthogonal codes with $\gamma < 1$ are found, but they require at least $\approx 2^{58}$ qubits. With CSS-T, codes it is possible to find codes with $\gamma < 1$ and a much lower number of qubits, for example the code $[[1024, 192, 8]]$ we showed before. The shorter CSS-T code that we find with $\gamma < 1$ is the code with parameters $[[256, 84, 4]]$, which has $\gamma = 0.804$. This shows that one can indeed obtain better parameters by relaxing the conditions on the classical codes and requiring them to be CSS-T instead of triorthogonal. We reiterate that this discussion is purely in terms of parameters, since triorthogonal codes implement the logical T gate, while for CSS-T codes we only require that they support a transversal T gate.

G.6 Conclusion

In this paper, we considered binary CSS-T codes, which are quantum stabilizer codes that respect a transversal gate. We provided a straightforward characterization of binary CSS-T codes and used it to demonstrate that CSS-T codes form a poset. We determined maximal and minimal elements of this poset as well as elements which are maximal with respect to one code in a CSS-T pair. We demonstrated a propagation rule for nondegenerate CSS-T codes. We used cyclotomic cosets to characterize CSS-T pairs from cyclic codes. Moreover, we obtained quantum codes with better parameters than those in the literature, using cyclic and extended cyclic codes. A number of related open problems remain, such as determining a similar characterizations of q-ary CSS-T codes and considering other families of classical codes to construct CSS-T codes.

G.7 Acknowledgements

Part of this work was done during the visit of Diego Ruano, Rodrigo San-José, and Ivan Soprunov to Virginia Tech. They thank Eduardo Camps Moreno, Hiram H. López, and Gretchen L. Matthews for their hospitality. The initial collaboration amongst the group (absent San-José) was facilitated by the Collaborate@ICERM program, supported by the National Science Foundation under Grant No. DMS-1929284.

Declarations

Conflict of interest

The authors declare no conflict of interest.

Bibliography

[1] J. T. Anderson, G. Duclos-Cianci, and D. Poulin. Fault-tolerant conversion between the Steane and Reed-Muller quantum codes. *Phys. Rev. Lett.*, 113:080501, Aug 2014.

[2] E. Andrade, J. Bolkema, T. Dexter, H. Eggers, V. Luongo, F. Manganiello, and L. Szramowski. CSS-T codes from Reed Muller codes for quantum fault tolerance. *ArXiv 2305.06423*, 2023.

[3] T. Ball, E. Camps, H. Chimal-Dzul, D. Jaramillo-Velez, H. López, N. Nichols, M. Perkins, I. Soprunov, G. Vera-Martínez, and G. Whieldon. Coding theory package for Macaulay2. *J. Softw. Algebra Geom.*, 11(1):113–122, 2021.

[4] E. Berardini, A. Caminata, and A. Ravagnani. Structure of CSS and CSS-T quantum codes. *Des. Codes Cryptogr.*, 2024.

[5] J. Bierbrauer. The theory of cyclic codes and a generalization to additive codes. *Des. Codes Cryptogr.*, 25(2):189–206, 2002.

[6] S. Bravyi and J. Haah. Magic-state distillation with low overhead. *Phys. Rev. A*, 86:052329, Nov 2012.

[7] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane. Quantum error correction via codes over GF(4). *IEEE Trans. Inform. Theory*, 44(4):1369–1387, 1998.

[8] A. R. Calderbank and P. W. Shor. Good quantum error-correcting codes exist. *Phys. Rev. A*, 54:1098–1105, Aug 1996.

[9] E. Camps-Moreno, H. H. López, G. L. Matthews, D. Ruano, R. San-José, and I. Soprunov. Parity check matrices for the codes in "An algebraic characterization of binary CSS-T codes and cyclic CSS-T codes for quantum fault tolerance". GitHub repository. Available online: `https://github.com/RodrigoSanJose/Cyclic-CSS-T`, 2024. Accessed on 18 April 2024.

[10] I. Cascudo. On squares of cyclic codes. *IEEE Trans. Inform. Theory*, 65(2):1034–1047, 2019.

[11] I. Cascudo, J. S. Gundersen, and D. Ruano. Squares of matrix-product codes. *Finite Fields Appl.*, 62:101606, 21, 2020.

[12] C. Galindo, F. Hernando, and D. Ruano. Stabilizer quantum codes from J-affine variety codes and a new Steane-like enlargement. *Quantum Inf. Process.*, 14(9):3211–3231, 2015.

[13] M. Grassl. Algebraic quantum codes: linking quantum mechanics and discrete mathematics. *International Journal of Computer Mathematics: Computer Systems Theory*, 6(4):243–259, 2021.

[14] M. Grassl. New quantum codes from CSS codes. *Quantum Inf. Process.*, 22(1):Paper No. 86, 11, 2023.

[15] D. R. Grayson and M. E. Stillman. Macaulay2, a software system for research in algebraic geometry.

[16] M. B. Hastings and J. Haah. Distillation with sublogarithmic overhead. *Phys. Rev. Lett.*, 120:050504, Jan 2018.

[17] S. Nezami and J. Haah. Classification of small triorthogonal codes. *Phys. Rev. A*, 106(1):Paper No. 012437, 13, 2022.

[18] D.-X. Quan, L.-L. Zhu, C.-X. Pei, and B. C. Sanders. Fault-tolerant conversion between adjacent Reed-Muller quantum codes based on gauge fixing. *J. Phys. A*, 51(11):115305, 16, 2018.

[19] E. M. Rains. Nonbinary quantum codes. *IEEE Trans. Inform. Theory*, 45(6):1827–1832, 1999.

[20] N. Rengaswamy, R. Calderbank, M. Newman, and H. D. Pfister. Classical coding problem from transversal T gates. In *2020 IEEE International Symposium on Information Theory (ISIT)*, pages 1891–1896, 2020.

[21] N. Rengaswamy, R. Calderbank, M. Newman, and H. D. Pfister. On optimality of CSS codes for transversal T. *IEEE J. Sel. Areas Inf. Theory*, 1(2):499–514, 2020.

[22] P. W. Shor. Scheme for reducing decoherence in quantum computer memory. *Phys. Rev. A*, 52:R2493–R2496, Oct 1995.

[23] A. Steane. Multiple-Particle Interference and Quantum Error Correction. *Proceedings of the Royal Society of London Series A*, 452(1954):2551–2577, Nov. 1996.

[24] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 10.3)*, 2023. `https://www.sagemath.org`.

Paper H

About the generalized Hamming weights of matrix-product codes

Rodrigo San-José

Abstract

We derive a general lower bound for the generalized Hamming weights of nested matrix-product codes, with a particular emphasis on the cases with two and three constituent codes. We also provide an upper bound which is reminiscent of the bounds used for the minimum distance of matrix-product codes. When the constituent codes are two Reed-Solomon codes, we obtain an explicit formula for the generalized Hamming weights of the resulting matrix-product code. We also deal with the non-nested case for the case of two constituent codes.

Keywords: Linear codes, Matrix-product codes, Generalized Hamming weights, Reed-Solomon codes.

MSC: 94B05, 94B65, 11T71.

DOI: 10.48550/arXiv.2407.11810

Reference: R. San-José. About the generalized Hamming weights of matrix-product codes. ArXiv 2407.11810 (2024).

Affiliation: Rodrigo San-José: IMUVA-Mathematics Research Institute, Universidad de Valladolid.

H.1 Introduction

The generalized Hamming weights (GHWs) of a linear code were introduced by Wei in [22], and they are a generalization of the minimum distance. As such, they give finer information about the code, and, in terms of applications, they characterize its performance on the wire-tap channel of type II and as a t-resilient function [22], and they also have applications to list decoding [7, 8]. These applications have motivated the study of these parameters for well known families of codes, such as Reed-Muller codes [9], Cartesian codes [2], hyperbolic codes [4], and algebraic geometry codes [1, 17], among others. Nevertheless, the computation of the GHWs of a code is, in general, a difficult problem, and they are still unknown for many families of codes.

Matrix-product codes (MPCs) were introduced by Blackmore and Norton in [3]. These codes have been object of study for many different applications [5, 6, 14, 15]. From the properties of the constituent codes, one can derive properties of the corresponding MPC. Most notably, one can obtain a lower bound for the minimum distance of the MPC from the minimum distance of the constituent codes [3], but one can also derive self-orthogonality properties for some matrices [6, 13, 16] or decoding algorithms [10–12].

The aim of this work is to study the GHWs of a MPC in terms of those of its constituent codes. By doing this, one can consider families of codes with known GHWs, and derive different codes with bounded GHWs using the MPC construction. This allows us to substantially expand the families of codes for which we have bounds for their GHWs. In Section H.3, we focus on the case of 2×2 matrices, without requiring the constituent codes to be nested. We give a lower bound for the GHWs of the corresponding MPC in terms of the GHWs of the constituent codes, and their sum and intersection. In Section H.4, by requiring the constituent codes to be nested, we generalize the techniques from Section H.3 to obtain a lower bound for the GHWs of an MPC for an arbitrary non-singular by columns (NSC) matrix, and, in Subsections H.4.1 and H.4.2, we describe it explicitly for the cases of two and three constituent codes. To complement these lower bounds, in Section H.5 we provide an upper bound for the GHWs of MPCs, which is reminiscent of the bound obtained for the minimum distance in [3]. In Section H.6, we apply our results for specific families of codes. In particular, we obtain the GHWs of the MPCs obtained by considering two Reed-Solomon codes and a 2×2 NSC matrix. We also test our bounds with Reed-Muller codes, which are sharp in all the cases we have checked with this family of codes.

H.2 Preliminaries

Let $\mathbb{F}_q$ be the finite field of q elements, where q is a power of a prime p. We start by defining MPCs as in [3].

Definition H.2.1. Let $C_1, \ldots, C_s \subset \mathbb{F}_q^n$ be linear codes of length n, which we call *constituent codes*, and let $A = (a_{ij}) \in \mathbb{F}_q^{s \times h}$ be an $s \times h$ matrix, with $s \leq h$. The *matrix-product code* associated to A and $C_1, \ldots, C_s$ is denoted $C = [C_1, \ldots, C_s] \cdot A$, and is the set of all matrix products $[v_1, \ldots, v_s] \cdot A$, where $v_i = (v_{1i}, \ldots, v_{ni})^t \in C_i$ is an $n \times 1$ column vector,

for $i = 1, \ldots, s$. Thus, the codewords of C are $n \times h$ matrices

$$c = \begin{pmatrix} v_{11}a_{11} + \cdots + v_{1s}a_{s1} & \cdots & v_{11}a_{1h} + \cdots + v_{1s}a_{sh} \\ \vdots & \ddots & \vdots \\ v_{n1}a_{11} + \cdots + v_{ns}a_{s1} & \cdots & v_{n1}a_{1h} + \cdots + v_{ns}a_{sh} \end{pmatrix}.$$

We regard C as a code of length nh by reading the entries of the matrix in column-major order. Hence, the codewords of C can be viewed as vectors of length nh

$$c = \left(\sum_{j=1}^{s} a_{j1}v_j, \ldots, \sum_{j=1}^{s} a_{jh}v_j \right) \in \mathbb{F}_q^{nh}. \tag{H.2.1}$$

For each vector $c \in C$, we have a natural subdivision of the coordinates in h blocks of length n, i.e.,

$$c = (c_1, c_2, \ldots, c_h),\ c_i \in \mathbb{F}_q^n.$$

Definition H.2.2. We denote by e_i, $1 \leq i \leq h$, the standard vectors of $\mathbb{Z}_2^h$. Let $y \in \mathbb{Z}_2^h$. Then we define

$$C(y) := \{c \in C \mid c_i = 0 \text{ for each } i \in \operatorname{supp}(y)\}.$$

In other words, $C(y)$ is similar to a shortening at the blocks given by $\operatorname{supp}(y)$, but without puncturing those coordinates.

Note that we are using subindices for vectors to express different things: to stress that a vector v_i belongs to C_i, to denote the i-th block c_i of a codeword $c \in C$, and to denote the standard vectors e_i of $\mathbb{Z}_2^h$. We will use different letters (v, c and e), which, together with the context, will help to clear any possible confusion.

With respect to the parameters of MPCs, it is clear that the length is nh, and the dimension is $k = k_1 + \cdots + k_s$, where $k_i = \dim C_i$, $1 \leq i \leq s$, if A has full rank. In what follows, we always assume that A has full rank. For the minimum distance, we have to introduce some notation. Let us denote by $R_i = (a_{i,1}, \ldots, a_{i,h})$ the element of $\mathbb{F}_q^h$ given by the i-th row of A, for $1 \leq i \leq s$. We denote by δ_i the minimum distance of the code C_{R_i} generated by $\langle R_1, \ldots, R_i \rangle$ in $\mathbb{F}_q^h$. In [19] it is proven that

$$d_1(C) \geq \min\{d_1(C_1)\delta_1, \ldots, d_1(C_s)\delta_s\}, \tag{H.2.2}$$

where $d_1(D)$ denotes the minimum distance the code D. Moreover, in [11], the authors prove that the previous bound is sharp if $C_s \subset \cdots \subset C_1$.

When working with MPCs, it is usual to consider the following condition, introduced in [3].

Definition H.2.3. Let A be an $s \times h$ matrix, and let A_t be the matrix formed by the first t rows of A. For $1 \leq j_i < \cdots < j_t \leq h$, we denote by $A(j_1, \ldots, j_t)$ the $t \times t$ matrix consisting of the columns $j_1, \ldots, j_t$ of A_t. A matrix A is *non-singular by columns* if $A(j_1, \ldots, j_t)$ is non-singular for each $1 \leq t \leq s$ and $1 \leq j_1 < \cdots < j_t \leq h$. In particular, an NSC matrix has full rank.

Example H.2.4. Let $\mathbb{F}_q = \{\beta_1, \ldots, \beta_q\}$. For $1 \leq s \leq q$, the Vandermonde matrix

$$V_m = \begin{pmatrix} 1 & \cdots & 1 \\ \beta_1 & \cdots & \beta_q \\ \vdots & \ddots & \vdots \\ \beta_1^{s-1} & \cdots & \beta_q^{s-1} \end{pmatrix}$$

is an NSC matrix. Also $V_M(j_1, \ldots, j_h)$ is NSC for any $s \leq h \leq q$ and $1 \leq j_1 < \cdots < j_h \leq q$.

In [3] it is shown that, if A is NSC, then the codes C_{R_i} are MDS, for $1 \leq i \leq s$. This implies that the bound (H.2.2) becomes

$$d_1(C) \geq \min\{hd_1(C_1), (h-1)d_1(C_2), \ldots, (h-s+1)d_1(C_s)\} \tag{H.2.3}$$

for the case of an NSC matrix.

One of the goals of this work is to generalize the bounds (H.2.2) and (H.2.3) to the case of the GHWs of C, which we introduce now. Let $D \subset C$ be a subcode. The support of D, denoted by $\mathrm{supp}(D)$, is defined as

$$\mathrm{supp}(D) := \{i \mid \exists\ u = (u_1, \ldots, u_{nh}) \in D,\ u_i \neq 0\}.$$

Note that, in this case, u_i is just the i-th coordinate of u, not the i-th block of length n of u. The r-th *generalized Hamming weight* of C, denoted by $d_r(C)$, is defined as

$$d_r(C) := \min\{|\mathrm{supp}(D)| \mid D \text{ is a subcode of } C \text{ with } \dim D = r\}.$$

Throughout the paper, we will denote $d_0(C) = 0$.

Remark H.2.5. Given a basis $B = \{b_1, \ldots, b_k\}$ for a subcode D, we have that

$$\mathrm{supp}(D) = \bigcup_{i=1}^{k} \mathrm{supp}(b_i).$$

The GHWs satisfy the following general properties for any linear code C, as shown in [22].

Theorem H.2.6 (Monotonicity)**.** *For an $[n, k]$ linear code C with $k > 0$ we have*

$$1 \leq d_1(C) < d_2(C) < \cdots < d_k(C) \leq n.$$

Corollary H.2.7 (Generalized Singleton Bound)**.** *For an $[n, k]$ linear code C we have*

$$d_r(C) \leq n - k + r,\ 1 \leq r \leq k.$$

We say that a code C is t-MDS if $d_t(C) = n - k + t$, for some $1 \leq t \leq \dim C$. If a code is t-MDS for $t < \dim C$, it is also $(t+1)$-MDS by Theorem H.2.6 and Corollary H.2.7. Thus, one usually studies what is the first t such that C is t-MDS.

Remark H.2.8. For an MDS code C, by Theorem H.2.6 and Corollary H.2.7 we have

$$d_r(C) = n - k + r,$$

for all $1 \leq r \leq k$.

Going back to MPCs, the block structure that we have allows us to divide the support of the code as follows.

Definition H.2.9. Let $C \subset \mathbb{F}_q^{nh}$. Then we define

$$\mathrm{supp}_i(C) := \mathrm{supp}(C) \cap \{(i-1)\cdot n + 1, \ldots, i \cdot n\},\ 1 \leq i \leq h.$$

It is clear that

$$\mathrm{supp}(C) = \bigcup_{i=1}^{h} \mathrm{supp}_i(C),$$

where the union is disjoint. This implies that

$$|\mathrm{supp}(C)| = \sum_{i=1}^{h} |\mathrm{supp}_i(C)|. \tag{H.2.4}$$

H.3 A bound for the GHWs of the MPCs with 2×2 matrices

In this section, we give a lower bound for the GHWs of MPCs obtained with a 2×2 matrix A, which we also assume to be NSC. If we denote

$$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix},$$

since A is NSC, we have $a_{1j} \neq 0$, $1 \leq j \leq 2$. Moreover, we also cannot have $a_{21} = a_{22} = 0$. Since exchanging the order of the columns of A produces a permutation equivalent MPC code, we will assume that $a_{22} \neq 0$. We give now the main result of the section, bounding from below the GHWs of a MPC in terms of the GHWs of sums and intersections of the constituent codes.

Theorem H.3.1. *Let $C_1, C_2 \subset \mathbb{F}_q^n$, and let $C = [C_1, C_2] \cdot A$, with A as above. Let $1 \leq r \leq \dim C$ and consider*

$$Y = \left\{ (\alpha_1, \alpha_2) : \begin{array}{c} \max\{r - \dim(C_1 + C_2), 0\} \leq \alpha_1 \leq \min\{\dim C_2, r\} \\ \max\{r - \dim(C_1 + C_2), 0\} \leq \alpha_2 \leq \min\{\dim(C_1 \cap C_2), r\} \\ \alpha_1 + \alpha_2 \leq r \end{array} \right\}.$$

Then

$$d_r(C) \geq \min_{(\alpha_1,\alpha_2)\in Y} B_{\alpha_1,\alpha_2},$$

where

$$B_{\alpha_1,\alpha_2} = \max\{d_{r-\alpha_1}(C_1 + C_2), d_{\alpha_2}(C_1 \cap C_2)\} + \max\{d_{r-\alpha_2}(C_1 + C_2), d_{\alpha_1}(C_2)\}.$$

Proof. Let $D \subset C$ with $\dim D = r$. We will associate a pair (α_1, α_2) to D, and we will see that

$$|\mathrm{supp}(D)| \geq B_{\alpha_1,\alpha_2}.$$

We consider the following subcodes of D (recall Definition H.2.2):

$$D_1 = D(e_1),\ D_2 = D(e_2),\ \text{and}\ D_3 = D/(D(e_1) + D(e_2)),$$

where D_3 is regarded as a subcode of D by fixing some set of representatives of the quotient vector space. It is clear that

$$D = D_1 \oplus D_2 \oplus D_3.$$

If we denote $\alpha_1 = \dim D_1$ and $\alpha_2 = \dim D_2$, we have that $\dim D_3 = r - \alpha_1 - \alpha_2 \geq 0$. Moreover, by (H.2.4), we have

$$|\mathrm{supp}(D)| = \sum_{i=1}^{2} |\mathrm{supp}_i(D)|.$$

Now we will bound $|\mathrm{supp}_i(D)|$ from below, for $1 \leq i \leq 2$. Let $i = 1$ (it is analogous for $i = 2$). We consider a basis $\mathcal{B}$ for D given by the union of some bases for D_1, D_2 and D_3, which we denote by $\mathcal{B}_1$, $\mathcal{B}_2$ and $\mathcal{B}_3$, respectively. We can use Remark H.2.5, and notice that

$$\mathrm{supp}_1(D_1) = \bigcup_{b \in \mathcal{B}_1} \mathrm{supp}_i(b) = \emptyset.$$

Therefore, $\mathrm{supp}_1(D) = \mathrm{supp}_1(D_2 \oplus D_3)$. Now we have two ways to bound $|\mathrm{supp}_1(D_2 \oplus D_3)|$:

(a) We consider the set

$$\mathcal{B}' := \{c_1 \mid c = (c_1, c_2) \in \mathcal{B}_2 \cup \mathcal{B}_3\},$$

that is, the set formed by the first block of the vectors in $\mathcal{B}_2 \cup \mathcal{B}_3$, which has size $r - \alpha_1$. From the definition of MPCs (see (H.2.1)), $\mathcal{B}' \subset C_1 + C_2$. Moreover, $\mathcal{B}'$ is a linearly independent set because, otherwise, we would have a linear combination of vectors of $\mathcal{B}_2 \cup \mathcal{B}_3$ in D_1, a contradiction. Thus,

$$|\mathrm{supp}_1(D)| = |\mathrm{supp}_1(D_2 \oplus D_3)| \geq d_{r-\alpha_1}(C_1 + C_2).$$

(b) We consider the set

$$\mathcal{B}'' = \{c_1 \mid c = (c_1, c_2) \in \mathcal{B}_2\}.$$

As the vectors of $\mathcal{B}_2$ are linearly independent and they have $c_2 = 0$, the vectors in $\mathcal{B}''$ are linearly independent. Let $c_1 \in \mathcal{B}''$. Then

$$(c_1, 0) = [v_1, v_2] \cdot A = (a_{11}v_1 + a_{21}v_2, a_{12}v_1 + a_{22}v_2),$$

for some $v_1 \in C_1$, $v_2 \in C_2$. Hence,

$$0 = a_{12}v_1 + a_{22}v_2 \implies v_1 = (-a_{22}/a_{12})v_2,$$

since $a_{12} \neq 0$. We are assuming $a_{22} \neq 0$, which implies $v_1, v_2 \in C_1 \cap C_2$. Therefore, $c_1 = a_{11}v_1 + a_{21}v_2 \in C_1 \cap C_2$ and $\mathcal{B}'' \subset C_1 \cap C_2$. We have obtained

$$|\mathrm{supp}_1(D)| = |\mathrm{supp}_1(D_2 \oplus D_3)| \geq d_{\alpha_2}(C_1 \cap C_2).$$

Using both bounds, we get

$$|\mathrm{supp}_1(D)| \geq \max\{d_{r-\alpha_1}(C_1 + C_2), d_{\alpha_2}(C_1 \cap C_2)\}.$$

An analogous argument applies to $\mathrm{supp}_2(D)$, taking into account that a_{21} can be zero. This means that in (b) we can only argue that $v_1, v_2 \in C_2$. We obtain the bound

$$|\mathrm{supp}_2(D)| \geq \max\{d_{r-\alpha_2}(C_1 + C_2), d_{\alpha_1}(C_2)\}.$$

Thus,

$$|\mathrm{supp}(D)| = |\mathrm{supp}_1(D)| + |\mathrm{supp}_2(D)| \geq B_{\alpha_1,\alpha_2}.$$

For any subcode D, from the arguments in (a) and (b) we deduce that the parameters $\alpha_1 = \dim D(e_1)$ and $\alpha_2 = \dim D(e_2)$ satisfy $(\alpha_1, \alpha_2) \in Y$, which concludes the proof. □

We have given the bound in the most general form. However, depending on whether a_{21} is zero or not, it is possible to improve the bound from the previous result, as we show next.

Corollary H.3.2. *With the notation as before, if $a_{21} \neq 0$, we can consider*

$$Y = \left\{ (\alpha_1, \alpha_2) : \begin{array}{c} \max\{r - \dim(C_1 + C_2), 0\} \leq \alpha_i \leq \min\{\dim C_1 \cap C_2, r\},\ 1 \leq i \leq 2 \\ \alpha_1 + \alpha_2 \leq r \end{array} \right\}.$$

Then

$$d_r(C) \geq \min_{(\alpha_1,\alpha_2)\in Y} B_{\alpha_1,\alpha_2},$$

where

$$B_{\alpha_1,\alpha_2} = \max\{d_{r-\alpha_1}(C_1 + C_2), d_{\alpha_2}(C_1 \cap C_2)\} + \max\{d_{r-\alpha_2}(C_1 + C_2), d_{\alpha_1}(C_1 \cap C_2)\}.$$

On the other hand, if $a_{21} = 0$, we can consider instead

$$Y = \left\{ (\alpha_1, \alpha_2) : \begin{array}{c} \max\{r - \dim(C_1), 0\} \leq \alpha_1 \leq \min\{\dim C_2, r\} \\ \max\{r - \dim(C_1 + C_2), 0\} \leq \alpha_2 \leq \min\{\dim C_1 \cap C_2, r\} \\ \alpha_1 + \alpha_2 \leq r \end{array} \right\}.$$

Then

$$d_r(C) \geq \min_{(\alpha_1,\alpha_2)\in Y} B_{\alpha_1,\alpha_2},$$

where

$$B_{\alpha_1,\alpha_2} = \max\{d_{r-\alpha_1}(C_1), d_{\alpha_2}(C_1 \cap C_2)\} + \max\{d_{r-\alpha_2}(C_1 + C_2), d_{\alpha_1}(C_2)\}.$$

Proof. In both cases we follow the proof from Theorem H.3.1. If $a_{21} \neq 0$, then in (b) we have $v_1, v_2 \in C_1 \cap C_2$ for both blocks $i = 1, 2$. If $a_{21} = 0$, then for any $c \in C$, we have $c_1 \in C_1$, improving the bound obtained in (a) for the first block. □

Remark H.3.3. The ideas in this section are a generalization of the ideas from [21], where the author considers a particular generator matrix for any subcode of a projective Reed-Muller code that is given by two parameters, α and γ. Those parameters play the role of $r - \alpha_2$ and α_1, respectively, in this section.

Note that, if $C_2 \subset C_1$, then all the bounds given in this section coincide. However, as we show in the next example, if we do not have this nested condition, then we can obtain different bounds in Corollary H.3.2. Moreover, in the next example we also show that, if the codes are not nested, our bounds can refine the usual bounds for the minimum distance of the $(u, u+v)$ and $(u+v, u-v)$ constructions by considering $d_1(C_1+C_2)$ and $d_1(C_1 \cap C_2)$.

Example H.3.4. Let $q = 3$, and consider

$$G_1 = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ -1 & 1 & 0 & 1 & -1 & 1 & 0 & 1 \\ -1 & 1 & -1 & 1 & 1 & 1 & 1 & 0 \end{pmatrix}, \; G_2 = \begin{pmatrix} -1 & 0 & 1 & 1 & -1 & 1 & -1 & 0 \\ 1 & 1 & 0 & 1 & -1 & -1 & -1 & -1 \end{pmatrix}.$$

Let C_1 and C_2 be the linear codes whose generator matrices are G_1 and G_2. Then, one can check that $C_1 \cap C_2 = \{0\}$, and the GHWs of C_1, C_2 and $C_1 + C_2$ are given in Table H.1.

Table H.1: GHWs of C_1, C_2 and $C_1 + C_2$

GHWs$\backslash r$	1	2	3	4	5
$d_r(C_1)$	3	6	8	-	-
$d_r(C_2)$	5	8	-	-	-
$d_r(C_1 + C_2)$	3	5	6	7	8

Now consider the matrices

$$A_1 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \; A_2 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix},$$

which correspond to the $(u, u+v)$ and $(u+v, u-v)$ constructions, respectively. Let $D_1 = [C_1, C_2] \cdot A_1$, $D_2 = [C_1, C_2] \cdot A_2$. The usual bounds for the minimum distance of D_1 and D_2 would give $\min\{2d_1(C_1), d_1(C_2)\} = 5$ (see [20, Thm. 2.1.32 & Prop. 2.1.39]). However, our bounds from Corollary H.3.2 give the values from Table H.2.

Table H.2: Lower bounds from Corollary H.3.2

Bound$\backslash r$	1	2	3	4	5
Lower bound for D_1	5	8	11	14	16
Lower bound for D_2	6	10	12	14	16

Note that the bound for $d_1(D_2)$ has been improved to 6. Also, notice that the bounds obtained from Corollary H.3.2 are different in this case for A_1 and A_2. This is noteworthy since, as we said before, the usual bounds for the minimum distance of the $(u, u+v)$ construction and the $(u+v, u-v)$ construction are the same. The true values of the GHWs are given in Table H.3, showing that our bounds are sharp in this case, except in the case $r = 4$ for D_2.

In this case, since $C_1 \cap C_2 = \{0\}$, the lower bounds from Corollary H.3.2 are particularly easy to compute. Indeed, if $a_{21} \neq 0$ (the case of A_2), we have $Y = \{(0,0)\}$. Thus, the bound is just

$$d_r(D_2) \geq B_{0,0} = 2d_r(C_1 + C_2).$$

Table H.3: GHWs of D_1 and D_2

GHWs\r	1	2	3	4	5
$d_r(D_1)$	5	8	11	14	16
$d_r(D_2)$	6	10	12	15	16

For the case $a_{21} = 0$, we obtain $Y = \{(\alpha_1, 0) \mid \max\{r-3, 0\} \leq \alpha_1 \leq \min\{2, r\}\}$, and

$$d_r(D_1) \geq \min_{(\alpha_1,0)\in Y} B_{\alpha_1,0} = \min_{(\alpha_1,0)\in Y} \{d_{r-\alpha_1}(C_1) + \max\{d_r(C_1+C_2), d_{\alpha_1}(C_2)\}\}.$$

For example, for $r = 3$, we have $Y = \{(0,0), (1,0), (2,0)\}$, and

$$d_3(D_1) \geq \min\{8 + \max\{3,0\}, 6 + \max\{6,5\}, 3 + \max\{6,8\}\} = 11.$$

H.4 A bound for the GHWs of nested MPCs with NSC matrices

In this section, we will show how to obtain a lower bound for the GHWs of MPCs with s constituent codes. We will assume that the codes are nested, i.e., $C_s \subset \cdots \subset C_1 \subset \mathbb{F}_q^n$. We consider A an $s \times h$ NSC matrix over $\mathbb{F}_q$ with $s \leq h$. By [3, Prop. 3.3], this implies that $h \leq q$. Let $C = [C_1, \ldots, C_s] \cdot A$. Let $D \subset C$ be a subcode of dimension r, for some $1 \leq r \leq \dim(C) = \sum_{i=1}^{s} \dim(C_i)$. From [15, Lem. 6] we have the following result.

Lemma H.4.1. *Let $C_s \subset \cdots \subset C_1 \subset \mathbb{F}_q^n$ and A an $s \times h$ NSC matrix over $\mathbb{F}_q$. Let $C = [C_1, \ldots, C_s] \cdot A$ and $c \in C$. We consider the h blocks of length n of c, that is, $c = (c_1, \ldots, c_h)$. Let $0 \leq \ell \leq s-1$. If there are exactly ℓ zero vectors among the blocks $c_1, \ldots, c_h$, then $c_j \in C_{\ell+1}$, for every $1 \leq j \leq h$. If the number of zero vectors among $c_1, \ldots, c_h$ is greater than $s-1$, then $c = 0$.*

Using this result, we will bound $|\mathrm{supp}_i(D)|$ for each $1 \leq i \leq h$, thus giving a bound for $|\mathrm{supp}(D)|$ (see (H.2.4)), as we did in the previous section,. For each block i, we can provide bounds looking at different subcodes of D. In what follows we fix some $1 \leq i \leq h$. First, let us consider

$$D/D(e_i).$$

We consider a basis for this quotient vector space, and fix representatives to obtain a set $\mathcal{B}_0^i \subset D$ which is linearly independent with size $\dim D/D(e_i) = r - \dim D(e_i)$. Moreover, let

$$\mathcal{B}_{0,i}^i := \{b_i \mid b \in \mathcal{B}_0^i\},$$

that is, the set formed by the i-th blocks of the vectors in $\mathcal{B}_0^i$. Note that $\mathcal{B}_{0,i}^i$ is linearly independent as well, since, if it were linearly dependent, then we would obtain a linear combination of vectors from $\mathcal{B}_0^i$ in $D(e_i)$, a contradiction because their classes are linearly independent in $D/D(e_i)$. Moreover, by Lemma H.4.1 (or the definition of MPCs), we have $\mathcal{B}_{0,i}^i \subset C_1$. Thus,

$$|\mathrm{supp}_i(D)| \geq \left| \bigcup_{b\in\mathcal{B}_0^i} \mathrm{supp}_i(b) \right| \geq d_{r-\dim D(e_i)}(C_1) = d_{|\mathcal{B}_0^i|}(C_1).$$

For this bound, we have considered codewords of D such that their i-th block is nonzero. Next, we consider codewords of $c \in D$ with $c_i \neq 0$ which can be generated by codewords with at least one zero block. This leads to considering

$$(\sum_{j=1}^{h} D(e_i))/D(e_i). \tag{H.4.1}$$

As before, we consider $\mathcal{B}_1^i \subset D$ a set of representatives for a basis of this quotient vector space, and we can assume that each representative is in some $D(e_j)$, $j \neq i$. Indeed, since the union of the bases of $D(e_i)$ is a generating set for $\sum_{j=1}^{h} D(e_i)$, the classes of the corresponding vectors form generating set of the quotient (H.4.1), and we can extract a basis from this generating set. In this way, we obtain a set of $\left|\mathcal{B}_1^i\right| = \dim(\sum_{j=1}^{h} D(e_i))/D(e_i) = \dim(\sum_{j=1}^{h} D(e_i)) - \dim D(e_i)$ linearly independent vectors, and each vector is in some $D(e_j)$, $j \neq i$, that is, it has at least one zero block. Moreover, arguing as before, if we restrict these vectors to the i-th block (the corresponding set is denoted $\mathcal{B}_{1,i}^i$), they are still linearly independent, and by Lemma H.4.1, we have $\mathcal{B}_{1,i}^i \subset C_2$. Hence, we obtain a second bound

$$|\mathrm{supp}_i(D)| \geq \left| \bigcup_{b \in \mathcal{B}_1^i} \mathrm{supp}_i(b) \right| \geq d_{\left|\mathcal{B}_1^i\right|}(C_2).$$

We can iterate this and obtain more bounds as follows. For $0 \leq j \leq s-1$, we can consider the codewords c with $c_i \neq 0$ and which can be generated by codewords with at least j zero blocks. In other words, we consider

$$\left(D(e_i) + \sum_{y \in \mathbb{Z}_2^h,\, \mathrm{wt}(y)=j} D(y) \right) \Big/ D(e_i). \tag{H.4.2}$$

Indeed, since $D(y) \subset D(e_i)$ if $y_i = 1$, we have

$$D(e_i) + \sum_{y \in \mathbb{Z}_2^h,\, \mathrm{wt}(y)=j} D(y) = D(e_i) + \sum_{y \in \mathbb{Z}_2^h,\, \mathrm{wt}(y)=j,\, y_i=0} D(y).$$

Thus, we can consider a basis for this last vector space where every vector is either in some $D(y)$, with $\mathrm{wt}(y) = j$, $y_i = 0$, or in $D(e_i)$. The classes of these vectors in (H.4.2) form a generating set, from which we can extract a basis $\mathcal{B}_j^i$ (regarded in $\mathbb{F}_q^{hn}$ by fixing some representatives) where every vector is in some $D(y)$, with $\mathrm{wt}(y) = j$, and is not contained in $D(e_i)$. That is, each vector of $\mathcal{B}_j^i$ has at least j zero blocks, and its i-th block is nonzero. The size of this set is

$$\begin{aligned} \left|\mathcal{B}_j^i\right| &= \dim \left(D(e_i) + \sum_{y \in \mathbb{Z}_2^h,\, \mathrm{wt}(y)=j} D(y) \right) \Big/ D(e_i). \\ &= \dim \left(\sum_{y \in \mathbb{Z}_2^h,\, \mathrm{wt}(y)=j} D(y) \right) - \dim \left(D(e_i) \cap \left(\sum_{y \in \mathbb{Z}_2^h,\, \mathrm{wt}(y)=j} D(y) \right) \right). \end{aligned} \tag{H.4.3}$$

Moreover, the vectors in $\mathcal{B}_j^i$ are linearly independent, and, arguing as before, the set of their i-th blocks, denoted $\mathcal{B}_{j,i}^i$, is also linearly independent. By Lemma H.4.1, $\mathcal{B}_{j,i}^i \subset C_{j+1}$, and

$$|\mathrm{supp}_i(D)| \geq \left| \bigcup_{b \in \mathcal{B}_j^i} \mathrm{supp}_i(b) \right| \geq d_{|\mathcal{B}_j^i|}(C_{j+1}).$$

Therefore, in this way we obtain s lower bounds for the i-th block. We can repeat this for every block i, $1 \leq i \leq h$, obtaining the bound

$$|\mathrm{supp}(D)| \geq \sum_{i=1}^{h} \max\{d_{|\mathcal{B}_j^i|}(C_{j+1}),\ 0 \leq j \leq s-1\}. \tag{H.4.4}$$

To bound the minimum of $|\mathrm{supp}(D)|$ for every $D \subset C$ with $\dim D = r$, the strategy we followed in Section H.3 was to determine all the possible values of $\left|\mathcal{B}_j^i\right|$ (which can be obtained from Y in Theorem H.3.1), and compute the minimum of the right hand side of (H.4.4) over all those values. The resulting bound would be

$$d_r(C) \geq \min_{D \subset C,\, \dim D = r} \left(\sum_{i=1}^{h} \max\{d_{|\mathcal{B}_j^i|}(C_{j+1}),\ 0 \leq j \leq s-1\} \right). \tag{H.4.5}$$

Remark H.4.2. For the case $r = 1$, this bound generalizes the bound from (H.2.3). Indeed, let $D \subset C$ with $\dim D = 1$, and consider i, j such that $\left|\mathcal{B}_j^i\right| = 1$ (since $r = 1$, $\left|\mathcal{B}_j^i\right|$ is either 0 or 1, and if all of them are 0, this would correspond to the subcode $D = \{0\}$). This means that D is generated by a vector c with at least j zero blocks, and with a nonzero i-th block. Let

$$j' := |\{k \mid c_k = 0\}|,$$

that is, the number of zero blocks of c. Then $\left|\mathcal{B}_{j'}^i\right| = 1$ since we can assume $\mathcal{B}_{j'}^i = \{c\}$. It follows from the definitions that, in this case, we have

$$\left|\mathcal{B}_k^i\right| = 1 \iff k \leq j',\ c_i \neq 0,$$

and, thus, $\left|\mathcal{B}_k^i\right| = 0$ otherwise. Then, for any i such that $c_i \neq 0$, we have

$$\max\{d_{|\mathcal{B}_j^i|}(C_{j+1}),\ 0 \leq j \leq s-1\} = \max\{d_1(C_1), \ldots, d_1(C_{j'+1})\} = d_1(C_{j'+1}).$$

Since c has exactly $h - j'$ nonzero blocks, we obtain

$$\sum_{i=1}^{h} \max\{d_{|\mathcal{B}_j^i|}(C_{j+1}),\ 0 \leq j \leq s-1\} = (h - j')d_1(C_{j'+1}),$$

which shows that the bound from (H.4.5) simplifies to (H.2.3) in this case.

The relations between the sizes of the $\mathcal{B}_j^i$ become increasingly more involved when considering greater values of s, which is what we need to determine Y. The main problem that arises is the fact that there is no inclusion-exclusion principle formula for the dimension

of the sum of vector spaces (e.g., note (H.4.3)). This means that there is no direct way to express the dimensions of the $\mathcal{B}_i^j$ in terms of the dimensions of the $D(y)$, for $y \in \mathbb{Z}_2^h$, as we did in Section H.3.

By introducing extra parameters corresponding to the dimension of sums of the $D(y)$ and their intersections with some other $D(y')$, $y, y' \in \mathbb{Z}_2^h$, and by taking into account the relations between these parameters, it is possible, in principle, to obtain a lower bound for any s and h ($s \leq h$), but the number of parameters required increases exponentially.

Since the cases that are more used for applications of MPCs involve only two or three codes, in the next subsections we show how to use these ideas to derive a more manageable lower bound for the GHWs of C when $s = 2$ or $s = 3$. The approach is the following. We will consider a set Y, and family of bounds $\{B_v\}_{v \in Y}$, such that for any subcode $D \subset C$ with $\dim D = r$, we have

$$\sum_{i=1}^{h} \max\{d_{|\mathcal{B}_j^i|}(C_{j+1}),\ 0 \leq j \leq s-1\} = B_v,$$

for some $v \in Y$. Therefore, from (H.4.5) we obtain

$$d_r(C) \geq \min_{D \subset C,\, \dim D = r} \left(\sum_{i=1}^{h} \max\{d_{|\mathcal{B}_j^i|}(C_{j+1}),\ 0 \leq j \leq s-1\} \right) \geq \min_{v \in Y} B_v. \tag{H.4.6}$$

H.4.1 The case $h = 2$

With the arguments from above, for the case $s = h = 2$ we can recover what we obtained in Section H.3 for the nested case.

Corollary H.4.3. *Let $C_2 \subset C_1 \subset \mathbb{F}_q^n$, $C = [C_1, C_2] \cdot A$, for some 2×2 NSC matrix A. Consider $1 \leq r \leq \dim C_1 + \dim C_2$, and let*

$$Y = \left\{ (\alpha_1, \alpha_2) : \begin{array}{c} \max\{r - \dim C_1, 0\} \leq \alpha_i \leq \min\{\dim C_2, r\},\ 1 \leq i \leq 2 \\ \alpha_1 + \alpha_2 \leq r \end{array} \right\}.$$

We consider

$$B_{\alpha_1,\alpha_2} = \max\{d_{r-\alpha_1}(C_1), d_{\alpha_2}(C_2)\} + \max\{d_{r-\alpha_2}(C_1), d_{\alpha_1}(C_2)\}.$$

Then

$$d_r(C) \geq \min_{(\alpha_1,\alpha_2) \in Y} B_{\alpha_1,\alpha_2}.$$

Proof. Let $D \subset C$ with $\dim D = r$. We apply the general argument that led to (H.4.5), considering $\alpha_i = \dim D(e_i)$, $1 \leq i \leq 2$, and taking into account that $\left|B_0^i\right| = r - \alpha_{i+1}$ (we consider $i + 1 \bmod 2$ for the subindex), $\left|B_1^i\right| = \alpha_i$. The first set of conditions about α_i, $1 \leq i \leq 2$, follow from the fact that $\mathcal{B}_{j,i}^i \subset C_{j+1}$ and $\left|\mathcal{B}_j^i\right| = \left|\mathcal{B}_{j,i}^i\right|$, for $j = 0, 1$. The condition $\alpha_1 + \alpha_2 \leq r$ arises from the fact that $D(e_1) + D(e_2) \subset D$, and $D(e_1) \cap D(e_2) = \{0\}$. Therefore, by (H.4.6), we obtain the result. □

H.4.2 The case $h = 3$

We now apply our techniques to the case $s = h = 3$. Throughout this section, when a subindex is greater than 3, we consider its reduction modulo 3. For instance, for $i = 2$, we have $e_{i+1} + e_{i+2} = e_3 + e_1$. We denote $\mathbb{Z}^{3,3,1} := \mathbb{Z}^3_{\geq 0} \times \mathbb{Z}^3_{\geq 0} \times \mathbb{Z}_{\geq 0}$.

Theorem H.4.4. *Let $C_3 \subset C_2 \subset C_1 \subset \mathbb{F}_q^n$ and $C = [C_1, C_2, C_3] \cdot A$, for some 3×3 NSC matrix A. Consider $1 \leq r \leq \sum_{i=1}^3 \dim C_i$, and let*

$$Y = \left\{ (\alpha, \gamma, \beta) \in \mathbb{Z}^{3,3,1} : \begin{array}{c} 0 \leq \gamma_i \leq \dim C_3,\ 1 \leq i \leq 3 \\ \max\{r - \dim C_1, \gamma_{i+1} + \gamma_{i+2}\} \leq \alpha_i,\ 1 \leq i \leq 3 \\ \alpha_{i+1} + \alpha_{i+2} - \gamma_i \leq \beta,\ 1 \leq i \leq 3 \\ \beta \leq \min\left\{ \sum_{i=1}^3 (\alpha_i - \gamma_i), \dim C_2 + \min\{\alpha_i, 1 \leq i \leq 3\}, r \right\} \end{array} \right\}.$$

For $(\alpha, \gamma, \beta) \in Y$, we consider

$$B_{\alpha,\gamma,\beta} = \sum_{i=1}^3 \max\{d_{r-\alpha_i}(C_1), d_{\beta-\alpha_i}(C_2), d_{\gamma_i}(C_3)\}.$$

Then we have

$$d_r(C) \geq \min_{(\alpha,\gamma,\beta)\in Y} B_{\alpha,\gamma,\beta}.$$

Proof. Let $D \subset C$ with $\dim D = r$. We consider $\alpha_i = \dim D(e_i)$, $\gamma_i = \dim D(e_{i+1} + e_{i+2})$ and $\beta = \dim(\sum_{j=1}^3 D(e_j))$, for $1 \leq i \leq 3$. We claim

$$\left|\mathcal{B}^i_j\right| = \begin{cases} \dim D/D(e_i) = r - \alpha_i & \text{if } j = 0, \\ \dim(\sum_{k=1}^3 D(e_k))/D(e_i) = \beta - \alpha_i & \text{if } j = 1, \\ \dim(D(e_i) + \sum_{k<\ell} D(e_k + e_\ell))/D(e_i) = \gamma_i & \text{if } j = 2. \end{cases} \tag{H.4.7}$$

The cases $j = 0$ and $j = 1$ are straightforward. For $j = 2$, we have

$$D(e_i) + \sum_{k<\ell} D(e_k + e_\ell) = D(e_i) + D(e_{i+1} + e_{i+2})$$

since $D(e_i + e_j) \subset D(e_i)$, for any $j \neq i$. Taking into account that $D(e_i) \cap D(e_{i+1} + e_{i+2}) = D((1,1,1)) = \{0\}$, we have

$$\dim(D(e_i) + \sum_{k<\ell} D(e_k + e_\ell))/D(e_i) = \dim(D(e_i) + D(e_{i+1} + e_{i+2})) - \dim D(e_i) = \gamma_i.$$

Let $\alpha = (\alpha_1, \alpha_2, \alpha_3)$, and $\gamma = (\gamma_1, \gamma_2, \gamma_3)$. Now we check that $(\alpha, \gamma, \beta) \in Y$ (we want to use (H.4.6)). It is clear that $0 \leq \gamma_i$, and, since $\gamma_i = \left|\mathcal{B}^i_2\right| = \left|\mathcal{B}^i_{2,i}\right|$ and $\mathcal{B}^i_{2,i} \subset C_3$, we have $\gamma_i \leq \dim C_3$, for $1 \leq i \leq 3$. Similarly, we have $r - \alpha_i = \left|B^i_0\right|$, which implies $r - \alpha_i \leq \dim C_1$, i.e., $r - \dim C_1 \leq \alpha_i$, for $1 \leq i \leq 3$. Now we note that

$$D(e_i + e_{i+2}) + D(e_i + e_{i+1}) \subset D(e_i).$$

Taking into account that $D(e_i+e_{i+2})\cap D(e_i+e_{i+1})=D((1,1,1))=\{0\}$, we deduce that $\gamma_{i+1}+\gamma_{i+2}\leq\alpha_i$, $1\leq i\leq 3$. Regarding the first condition for β in Y, we note that

$$\beta=\dim\left(\sum_{i=1}^{3}D(e_i)\right)\geq\dim(D(e_{k+1})+D(e_{k+2}))=\alpha_{k+1}+\alpha_{k+2}-\gamma_k,$$

for $1\leq k\leq 3$. It is clear that $\beta\leq r$, and, since $\beta-\alpha_i=\left|\mathcal{B}_1^i\right|=\left|\mathcal{B}_{1,i}^i\right|$ and $\mathcal{B}_{1,i}^i\subset C_2$, we have $\beta-\alpha_i\leq\dim C_2$, $1\leq i\leq 3$. The last condition we need to prove is $\beta\leq\sum_{i=1}^{3}(\alpha_i-\gamma_i)$. Note that, using the formula for the dimension of the sum of vector spaces twice, we have

$$\dim\left(\sum_{i=1}^{3}D(e_i)\right)=\sum_{i=1}^{3}\alpha_i-\gamma_k-\dim(D(e_k)\cap(D(e_{k+1})+D(e_{k+2}))),$$

for any $1\leq k\leq 3$. Since $D(e_k+e_{k+1})+D(e_k+e_{k+2})\subset D(e_k)\cap(D(e_{k+1})+D(e_{k+2}))$, we conclude

$$\beta=\dim\left(\sum_{i=1}^{3}D(e_i)\right)\leq\sum_{i=1}^{3}\alpha_i-\gamma_k-(\gamma_{k+2}+\gamma_{k+1})=\sum_{i=1}^{3}(\alpha_i-\gamma_i).$$

Thus, we have proved that $(\alpha,\gamma,\beta)\in Y$ and, if we note the expressions in (H.4.5) and (H.4.7), we have also proved that

$$\sum_{i=1}^{3}\max\{d_{|\mathcal{B}_j^i|}(C_{j+1}),\ 0\leq j\leq 3-1\}=B_{\alpha,\gamma,\beta},$$

for some $(\alpha,\gamma,\beta)\in Y$. We obtain the result by (H.4.6). □

Remark H.4.5. As we have seen in the proof of the previous result, we have codified some of the relations between the dimensions of $D(e_i)$, $D(e_{i+1}+e_{i+2})$ and $\sum_{k=1}^{3}D(e_k)$, for $1\leq i\leq 3$, using α_i, γ_i and β, respectively. In fact, many of the relations between these dimensions that one could expect can be derived from the ones included in the definition of Y. For example, we have

$$\dim(D(e_i))+\dim(D(e_{i+1}+e_{i+2}))=\dim(D(e_i)+D(e_{i+1}+e_{i+2}))\leq\dim(\sum_{i=1}^{3}D(e_i)).$$

This means that we should have $\alpha_i+\gamma_i\leq\beta$, for $1\leq i\leq 3$. This is a consequence of the conditions we gave for Y because

$$\beta\geq\alpha_{i+1}+\alpha_{i+2}-\gamma_i\geq\alpha_{i+1}+\gamma_{i+1},\ 1\leq i\leq 3,$$

since we also impose the condition $\alpha_{i+2}\geq\gamma_i+\gamma_{i+1}$.

Theorem H.4.4 can also be used to give a bound for the GHWs in the case $s=2$, $h=3$, as the next result shows. In this case, we denote $\mathbb{Z}^{3,1}=\mathbb{Z}_{\geq 0}^3\times\mathbb{Z}_{\geq 0}$.

Corollary H.4.6. *Let $C_2 \subset C_1 \subset \mathbb{F}_q^n$, $C = [C_1, C_2] \cdot A$, for some 2×3 NSC matrix A. Let*

$$Y = \left\{ (\alpha, \beta) \in \mathbb{Z}^{3,1} : \begin{array}{c} \max\{r - \dim C_1, 0\} \leq \alpha_i,\ 1 \leq i \leq 3 \\ \alpha_{i+1} + \alpha_{i+2} \leq \beta,\ 1 \leq i \leq 3 \\ \beta \leq \min\left\{ \sum_{i=1}^{3} \alpha_i, \dim C_2 + \min\{\alpha_i, 1 \leq i \leq 3\}, r \right\} \end{array} \right\}.$$

For $(\alpha, \beta) \in Y$ we consider

$$B_{\alpha,\beta} = \sum_{i=1}^{3} \max\{d_{r-\alpha_i}(C_1), d_{\beta-\alpha_i}(C_2)\}.$$

Then we have

$$d_r(C) \geq \min_{(\alpha,\beta)\in Y} B_{\alpha,\beta}.$$

Proof. This can be obtained directly from Theorem H.4.4 by setting $C_3 = \{0\}$. □

Example H.4.7. Let $q = 4$ and $n = 4$. In this example (and throughout the rest of the paper) we denote by $\mathrm{RS}(k)$ the Reed-Solomon code of length n and dimension k. Note that, by Remark H.2.8, we know the GHWs of Reed-Solomon codes. Let $k_1 = 3$ and $k_2 = 1$. We will compute the bound from Corollary H.4.6 for the code $C = [\mathrm{RS}(k_1), \mathrm{RS}(k_2)] \cdot A$ and $r = 2$, where

$$A = \begin{pmatrix} 1 & a & 1 \\ 1 & 1 & 0 \end{pmatrix},$$

and where a is a primitive element of $\mathbb{F}_4$. We start by computing Y. First, we have $0 \leq \alpha_i \leq r = 2$, for $1 \leq i \leq 3$. For β, we have the conditions $\alpha_{i+1} + \alpha_{i+2} \leq \beta$, for $1 \leq i \leq 3$, and $\beta \leq \min\{\sum_{i=1}^{3} \alpha_i, 1 + \min\{\alpha_i, 1 \leq i \leq 3\}, 2\}$. It is straightforward to check that $\{(0,0,0)\} \times \{0\} \in Y$. If we consider $\alpha = (1,0,0)$, then, looking at the conditions for β, this implies $\beta = 1$, and we have $\{(1,0,0)\} \times \{1\} \in Y$. Similarly, we have $\{(0,1,0)\} \times \{1\}, \{(0,0,1)\} \times \{1\} \in Y$. Finally, if we consider $\alpha = (1,1,1)$, this implies $\beta = 2$ and $\{(1,1,1)\} \times \{2\} \in Y$. In fact, one can check that these are all the elements of Y. For example, if we consider $\alpha = (1,1,0)$, then we must have $\alpha_1 + \alpha_2 = 2 \leq \beta$, but also $\beta \leq 1 + \min\{\alpha_i, 1 \leq i \leq 3\} = 1$, a contradiction. A similar reasoning applies to $\alpha = (1,0,1)$ or $\alpha = (0,1,1)$, and also for the cases where $\alpha_i = 2$ for some $1 \leq i \leq 3$.

Therefore, we have

$$Y = \{\{(0,0,0)\} \times \{0\}, \{(1,0,0), (0,1,0), (0,0,1)\} \times \{1\}, \{(1,1,1)\} \times \{2\}\}.$$

Now we compute $B_{\alpha,\beta}$, for each $(\alpha, \beta) \in Y$:

$$B_{(0,0,0),0} = 3d_2(\mathrm{RS}(k_1)) = 3(n - k_1 + 2) = 9,$$
$$B_{(1,0,0),1} = B_{(0,1,0),1} = B_{(0,0,1),1} = d_1(\mathrm{RS}(k_1)) + 2\max\{d_2(\mathrm{RS}(k_1)), d_1(\mathrm{RS}(k_2))\} = 10,$$
$$B_{(1,1,1),1} = 3d_1(\mathrm{RS}(k_2)) = 3(n - k_2 + 1) = 12.$$

Hence, we obtain

$$d_2(C) \geq \min_{(\alpha,\beta)\in Y} B_{\alpha,\beta} = 9.$$

It can be checked with a computer that this is the true value of $d_2(C)$.

H.5 An upper bound for the GHWs

In this section we give an upper bound for the GHWs of MPCs, complementing the previous section, as this will allow us to ensure that our bound is sharp when both bounds coincide. For this result, we do not require A to be NSC. We recall that $R_i = (a_{i,1}, \dots, a_{i,h})$ is the i-th row of A, for $1 \leq i \leq s$; δ_i is the minimum distance of the code C_{R_i} generated by $\langle R_1, \dots, R_i \rangle$; and A_i is the matrix formed by the first i rows of A. The proof of the following result is a generalization of the proof in [11, Thm. 1] for the minimum distance.

Proposition H.5.1. *Let $C_s \subset \cdots \subset C_1 \subset \mathbb{F}_q^n$, and $C = [C_1, \dots, C_s] \cdot A$, where $A \subset \mathbb{F}_q^{s \times h}$ has full rank. Let $1 \leq r \leq \dim C_1$ and let $1 \leq i \leq s$ be such that $r \leq \dim C_i$. Then*

$$d_r(C) \leq d_r(C_i)\delta_i.$$

Proof. Let $1 \leq i \leq s$ be such that $r \leq \dim C_i$. We will obtain a subcode $D \subset C$ with $\dim D = r$ and $|\mathrm{supp}(D)| = d_r(C_i)\delta_i$. First, we consider a subcode $D_i \subset C_i$ with $\dim D_i = r$ and $|\mathrm{supp}(D_i)| = d_r(C_i)$. We also consider $f = \sum_{j=1}^{i} \lambda_j R_j$, with $\lambda_j \in \mathbb{F}_q$, a codeword of C_{R_i} with $\mathrm{wt}(f) = \delta_i$. Then we claim that

$$D := \{[\lambda_1 v_1, \dots, \lambda_i v_i, v_{i+1}, \dots, v_s] \cdot A \mid v_1 = v_2 = \cdots = v_i \in D_i, v_{i+1} = v_{i+2} = \cdots = v_s = 0\}$$

is a subcode of C with $\dim D = r$ and $|\mathrm{supp}(D)| = d_r(C_i) \cdot \delta_i$. It is clear that $D \subset C$ because $D_i \subset C_i \subset \cdots \subset C_1$, and $\dim D = r$ since A has full rank. Let $v \in D_i$, then

$$[\lambda_1 v, \dots, \lambda_i v] \cdot A_i = \left(\sum_{j=1}^{i} a_{j1}\lambda_j v, \dots, \sum_{j=1}^{i} a_{jh}\lambda_j v \right) = (vf_1, \dots, vf_h),$$

where $f = (f_1, \dots, f_h) \in \mathbb{F}_q^h$, that is, f_i is the i-th coordinate of f, for $1 \leq i \leq h$. Hence,

$$D = \{(vf_1, \dots, vf_h) \in C \mid v \in D_i\}.$$

From this expression and the fact that $|\mathrm{supp}(D_i)| = d_r(C_i)$, we obtain

$$\left|\mathrm{supp}_j(D)\right| = \begin{cases} d_r(C_i) & \text{if } f_j \neq 0, \\ 0 & \text{if } f_j = 0. \end{cases}$$

Since $\mathrm{wt}(f) = \delta_i$, we have $|\mathrm{supp}(D)| = d_r(C_i) \cdot \delta_i$. □

Remark H.5.2. In the previous result, if A is NSC, then by [3, Prop. 7.2] we have $\delta_i = (h - i + 1)$, $1 \leq i \leq h$. Moreover, if A is triangular (that is, a column permutation of an upper triangular matrix), then the previous result holds even if the codes are not nested (this was already known to be true for the minimum distance [3, Thm. 3.7]). Indeed, we just need to consider

$$D' := \{[v_1, \dots, v_s] \cdot A \mid v_i \in D_i,\ v_j = 0 \text{ if } j \neq i\},$$

where we consider D_i as in the proof of Proposition H.5.1. Since A is triangular, we have

$$D' = \{(a_{i1}v, \dots, a_{ih}v) \mid v \in D_i\},$$

where a_{ij} is nonzero for exactly $h - i + 1$ values of j, which implies $|\mathrm{supp}(D)| = d_r(C_i) \cdot \delta_i$.

Note that the previous result does not provide any upper bound if $r > \dim C_1$, and, when $r = \dim C_1$, it only gives $d_r(C) \leq h \cdot n = N$, which cannot be sharp if $\dim C_2 \geq 1$ due to the monotony of the GHWs. This contrasts with the case of the minimum distance ($r = 1$), where one gets that the minimum of the bounds provided in Proposition H.5.1 is always sharp [11, Thm. 1]. Nevertheless, for lower values of r, this bound performs well, as we see in the following example (and as we will see in Theorem H.6.1).

Example H.5.3. Using the setting from Example H.4.7, from Proposition H.5.1, we obtain

$$d_2(C) \leq 3d_2(\mathrm{RS}(k_1)) = 9.$$

Thus, from this we can also deduce that the bound given in Example H.4.7 is sharp.

H.6 Examples for particular families of codes

We start by considering Reed-Solomon codes $\mathrm{RS}(k)$ with dimension k and length $n \leq q$, for which we know the GHWs from Remark H.2.8. In what follows, we denote

$$d_r(\mathrm{RS}(k)) = \begin{cases} 0 & \text{if } r = 0 \\ n - k + r & \text{if } 1 \leq r \leq k, \\ \infty & \text{if } k < r. \end{cases} \tag{H.6.1}$$

Theorem H.6.1. *Let $1 \leq k_2 \leq k_1 \leq n \leq q$, let $A \subset \mathbb{F}_q^{2\times 2}$ be a NSC matrix, and let $\mathrm{RS}(k_1, k_2) := [\mathrm{RS}(k_1), \mathrm{RS}(k_2)] \cdot A$. For $1 \leq r \leq \dim \mathrm{RS}(k_1, k_2) = k_1 + k_2$, we have*

$$d_r(\mathrm{RS}(k_1, k_2)) = \begin{cases} 2n + r - (k_1 + k_2) & \text{if } r > \max\{k_1 - k_2, k_2\}, \\ \min\{2d_r(\mathrm{RS}(k_1)), d_r(\mathrm{RS}(k_2))\} & \text{if } r \leq \max\{k_1 - k_2, k_2\}. \end{cases}$$

Proof. Let $\alpha_i \neq 0$, $\alpha_i \neq r$, for $1 \leq i \leq 2$. First, we give a lower bound for $d_r(\mathrm{RS}(k_1, k_2))$ using Corollary H.4.3. By (H.6.1) we have

$$B_{\alpha_1,\alpha_2} = \sum_{i=1}^{2} \max\{n - k_1 + r - \alpha_i, n - k_2 + \alpha_{i+1}\},$$

where $i + 1$ is understood to be $i + 1 \bmod 2$. This can be expressed as

$$B_{\alpha_1,\alpha_2} = \begin{cases} 2(n - k_1 + r) - (\alpha_1 + \alpha_2) & \text{if } r \geq k_1 - k_2 + \alpha_1 + \alpha_2, \\ 2(n - k_2) + \alpha_1 + \alpha_2 & \text{if } r < k_1 - k_2 + \alpha_1 + \alpha_2. \end{cases} \tag{H.6.2}$$

We now study the minimum of B_{α_1,α_2} for all $(\alpha_1, \alpha_2) \in Y$, with $\alpha_i \neq 0$, $\alpha_i \neq r$, using this expression. Let $\xi := r - (k_1 - k_2)$, and $z = \alpha_1 + \alpha_2$. Consider $(\alpha_1, \alpha_2) \in Y$ with $\alpha_i \neq 0$, $\alpha_i \neq r$. Then we can rewrite (H.6.2) as

$$B(z) := B_{\alpha_1,\alpha_2} = \begin{cases} 2(n - k_2) + z & \text{if } z > \xi, \\ 2(n - k_1 + r) - z & \text{if } z \leq \xi. \end{cases}$$

As a function of z, we see that $B(z)$ is an increasing function for $z > \xi$ and a decreasing function for $z \leq \xi$. Thus, the minimum for $(\alpha_1, \alpha_2) \in Y$, $\alpha_i \neq 0$, $\alpha_i \neq r$, is always greater than or equal to

$$B(\xi) = 2n + r - (k_1 + k_2).$$

Now we study the minimum of B_{α_1,α_2} for $(\alpha_1, \alpha_2) \in Y$, $\alpha_1 = 0$, $0 < \alpha_2 < r$. As before, we can write

$$B_{0,\alpha_2} = \begin{cases} 2(n - k_1 + r) - \alpha_2 & \text{if } r \geq k_1 - k_2 + \alpha_2, \\ 2n + r - (k_1 + k_2) & \text{if } r < k_1 - k_2 + \alpha_2. \end{cases}$$

As a function of α_2, this is constant for $\alpha_2 > r - (k_1 - k_2)$, and it is decreasing for $\alpha_2 \leq r - (k_1 - k_2)$. The minimum over α_2, with $0 < \alpha_2 < r$, is greater than or equal to

$$B_{0,r-(k_1-k_2)} = 2n + r - (k_1 + k_2) = B(\xi)$$

The only cases left to check are $(\alpha_1, \alpha_2) = (0, 0)$ and $(\alpha_1, \alpha_2) = (0, r)$, if they are in Y (the rest of the cases are also covered by symmetry between α_1 and α_2). We have

$$B_{0,0} = 2(n - k_1 + r) = 2d_r(C_1),\ B_{0,r} = n - k_2 + r = d_r(C_2).$$

Note that $(0, 0) \in Y$ if and only if $r - k_1 \leq 0$, and $(0, r) \in Y$ if and only if $r - k_1 \leq 0$ and $r \leq k_2$ (this last condition implies $r \leq k_1$). It is straightforward to check that $B(\xi) \leq B_{0,0}$ if and only if $r \geq k_1 - k_2$, $B_{0,r} \leq B(\xi)$ always (but $(0, r) \in Y$ only if $r \leq k_2$), and $B_{0,0} \leq B_{0,r}$ if and only if $r \leq k_1 - k_2 - (n - k_1)$. Therefore, by Corollary H.4.3, we obtain

$$d_r(\mathrm{RS}(k_1, k_2)) \geq \begin{cases} B(\xi) & \text{if } r > \max\{k_1 - k_2, k_2\}, \\ d_r(C_2) & \text{if } k_1 - k_2 \leq k_2 \text{ and } k_1 - k_2 < r \leq k_2, \\ 2d_r(C_1) & \text{if } k_1 - k_2 > k_2 \text{ and } k_2 < r \leq k_1 - k_2, \\ d_r(C_2) & \text{if } k_1 - k_2 - (n - k_1) < r \leq \min\{k_1 - k_2, k_2\}, \\ 2d_r(C_1) & \text{if } r \leq k_1 - k_2 - (n - k_1). \end{cases} \tag{H.6.3}$$

It is straightforward to check that this lower bound is equal to the formula in the statement of the result (with the notation from (H.6.1)). By Proposition H.5.1 and Corollary H.2.7, the previous bound is sharp for $1 \leq r \leq \dim \mathrm{RS}(k_1, k_2)$. □

Remark H.6.2. Note that the previous result shows that $\mathrm{RS}(k_1, k_2)$ is t-MDS, for $t = \max\{k_1 - k_2, k_2\}$.

In a similar way, we can consider other families of nested codes for which we know the GHWs, for example Hermitian codes [1] or Cartesian codes [2]. However, obtaining an explicit result like Theorem H.6.1 seems out of reach since the expressions of the GHWs of these families of codes are more involved than those of Reed-Solomon codes.

We turn our attention now to the family of Reed-Muller codes, which is closely related to MPCs, as we see next. We denote by $\mathrm{RM}_q(\nu, m)$ the Reed-Muller code of degree ν in m variables over $\mathbb{F}_q$. We take $\mathbb{F}_q = \{\alpha_1, \ldots, \alpha_q\}$. Let

$$\binom{\alpha_j}{\alpha_i} := \frac{(\alpha_j - \alpha_1) \cdots (\alpha_j - \alpha_{i-1})}{(\alpha_i - \alpha_1) \cdots (\alpha_i - \alpha_{i-1})},$$

where we understand that if $i = 1$ or $i = j$ then $\binom{\alpha_j}{\alpha_i} = 1$, and $\binom{\alpha_j}{\alpha_i} = 0$ if and only if $1 \leq j \leq i-1$. We consider the matrix

$$\mathrm{GRM}_q := \begin{pmatrix} \binom{\alpha_1}{\alpha_1} & \binom{\alpha_2}{\alpha_1} & \cdots & \binom{\alpha_q}{\alpha_1} \\ \binom{\alpha_1}{\alpha_2} & \binom{\alpha_2}{\alpha_2} & \cdots & \binom{\alpha_q}{\alpha_2} \\ \vdots & \vdots & \ddots & \vdots \\ \binom{\alpha_1}{\alpha_q} & \binom{\alpha_2}{\alpha_q} & \cdots & \binom{\alpha_q}{\alpha_q} \end{pmatrix}.$$

In [3, Section 5], the authors prove that GRM_q is NSC, and they also prove the following result.

Theorem H.6.3. *The Reed-Muller codes can be recursively defined by*

$$\mathrm{RM}_q(\nu, 0) = \begin{cases} \{0\} & \text{if } r < 0, \\ \mathbb{F}_q & \text{if } r \geq 0, \end{cases}$$

and for $m \geq 1$

$$\mathrm{RM}_q(\nu, m) = [\mathrm{RM}_q(\nu, m-1), \cdots, \mathrm{RM}_q(\nu - q + 1, m-1)] \cdot \mathrm{GRM}_q\,. \tag{H.6.4}$$

For $q = 2$ and $q = 3$, we get

$$\mathrm{GRM}_2 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},\ \mathrm{GRM}_3 = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix}.$$

In particular, this recovers the well-known result that binary Reed-Muller codes can be constructed recursively using the $(u, u+v)$ construction.

Another important aspect of Reed-Muller codes in this context is that their GHWs are known [9]. Therefore, they provide a family in which to test our bounds, in particular Corollary H.4.3 and Theorem H.4.4. For example, for $q = 2$, we can bound the GHWs of $\mathrm{RM}_2(\nu, m)$ with Corollary H.4.3 using the GHWs of $\mathrm{RM}_2(\nu, m-1)$ and $\mathrm{RM}_2(\nu-1, m-1)$, and we can check if the bound is sharp because we know the true values of the GHWs of $\mathrm{RM}_2(\nu, m)$. We can proceed similarly for the case of $q = 3$ using Theorem H.4.4. Note that we can apply our results since GRM_q is NSC and $\mathrm{RM}_q(\nu_1, m) \subset \mathrm{RM}_q(\nu_2, m)$ if $\nu_1 \leq \nu_2$, i.e., the codes in (H.6.4) are nested.

For $2 \leq m \leq 10$, we have computed the bound from Corollary H.4.3 for $\mathrm{RM}_2(\nu, m)$, $0 \leq \nu \leq m(q-1)$, and we have checked that the bound coincides with the corresponding GHW. This not only shows that the bound from Corollary H.4.3 is sharp in this case, but also showcases the fact that it can be computed efficiently even for large codes.

For the case $q = 3$, we have computed the bound from Theorem H.4.4 for $2 \leq m \leq 3$ variables, which also gives the true value of the corresponding GHW of $\mathrm{RM}_3(\nu, m)$, $1 \leq \nu \leq m(q-1)$. Since this bound is more computationally intensive to compute than the one from Corollary H.4.4, is not feasible to compute it for every possible degree for a larger number of variables. Notwithstanding the foregoing, we have tested a wide range of degrees for 4 and 5 variables, and the bound is sharp for all of them.

Another family of codes which can be constructed recursively using the MPC construction is the family of Berman codes [18], which are nested, similarly to Reed-Muller codes. However, the matrices corresponding to these codes are not NSC. Thus, it would be interesting to see if some of the results from Section H.4 could be generalized to the case of general matrices A, but keeping the nested condition on the component codes.

Declarations

Conflict of interest

The author declares that he has no conflict of interest.

Bibliography

[1] A. I. Barbero and C. Munuera. The weight hierarchy of Hermitian codes. *SIAM J. Discrete Math.*, 13(1):79–104, 2000.

[2] P. Beelen and M. Datta. Generalized Hamming weights of affine Cartesian codes. *Finite Fields Appl.*, 51:130–145, 2018.

[3] T. Blackmore and G. H. Norton. Matrix-product codes over $\mathbb{F}_q$. *Appl. Algebra Engrg. Comm. Comput.*, 12(6):477–500, 2001.

[4] E. Camps-Moreno, I. García-Marco, H. H. López, I. Márquez-Corbella, E. Martínez-Moro, and E. Sarmiento. On the generalized Hamming weights of hyperbolic codes. *J. Algebra Appl.*, 23(7):Paper No. 2550062, 18, 2024.

[5] C. Galindo, F. Hernando, C. Munuera, and D. Ruano. Locally recoverable codes from the matrix-product construction. *ArXiv 2310.15703*, 2023.

[6] C. Galindo, F. Hernando, and D. Ruano. New quantum codes from evaluation and matrix-product codes. *Finite Fields Appl.*, 36:98–120, 2015.

[7] P. Gopalan, V. Guruswami, and P. Raghavendra. List decoding tensor products and interleaved codes. *SIAM J. Comput.*, 40(5):1432–1462, 2011.

[8] V. Guruswami. List decoding from erasures: bounds and code constructions. *IEEE Trans. Inform. Theory*, 49(11):2826–2833, 2003.

[9] P. Heijnen and R. Pellikaan. Generalized Hamming weights of q-ary Reed-Muller codes. *IEEE Trans. Inform. Theory*, 44(1):181–196, 1998.

[10] F. Hernando, T. Høholdt, and D. Ruano. List decoding of matrix-product codes from nested codes: an application to quasi-cyclic codes. *Adv. Math. Commun.*, 6(3):259–272, 2012.

[11] F. Hernando, K. Lally, and D. Ruano. Construction and decoding of matrix-product codes from nested codes. *Appl. Algebra Engrg. Comm. Comput.*, 20(5-6):497–507, 2009.

[12] F. Hernando and D. Ruano. Decoding of matrix-product codes. *J. Algebra Appl.*, 12(4):1250185, 15, 2013.

[13] S. Jitman and T. Mankean. Matrix-product constructions for Hermitian self-orthogonal codes. *Chamchuri J. Math.*, 9:35–51, 2017.

[14] G. Luo, M. F. Ezerman, and S. Ling. Three new constructions of optimal locally repairable codes from matrix-product codes. *IEEE Trans. Inform. Theory*, 69(1):75–85, 2023.

[15] G. Luo, M. F. Ezerman, S. Ling, and X. Pan. New families of MDS symbol-pair codes from matrix-product codes. *IEEE Trans. Inform. Theory*, 69(3):1567–1587, 2023.

[16] T. Mankean and S. Jitman. Matrix-product constructions for self-orthogonal linear codes. In *2016 12th International Conference on Mathematics, Statistics, and Their Applications (ICMSA)*, pages 6–10, 2016.

[17] C. Munuera. On the generalized Hamming weights of geometric Goppa codes. *IEEE Trans. Inform. Theory*, 40(6):2092–2099, 1994.

[18] L. P. Natarajan and P. Krishnan. Berman codes: a generalization of Reed-Muller codes that achieve BEC capacity. *IEEE Trans. Inform. Theory*, 69(11):6956–6980, 2023.

[19] F. Özbudak and H. Stichtenoth. Note on Niederreiter-Xing's propagation rule for linear codes. *Appl. Algebra Engrg. Comm. Comput.*, 13(1):53–56, 2002.

[20] R. Pellikaan, X.-W. Wu, S. Bulygin, and R. Jurrius. *Codes, cryptology and curves with computer algebra*. Cambridge University Press, Cambridge, 2018.

[21] R. San-José. A recursive construction for projective Reed-Muller codes. *IEEE Transactions on Information Theory, to appear. ArXiv 2312.05072*, 2024.

[22] V. K. Wei. Generalized Hamming weights for linear codes. *IEEE Trans. Inform. Theory*, 37(5):1412–1418, 1991.

Part III

Conclusion

Conclusion

In this thesis we have studied several interactions between Commutative Algebra and Coding Theory, with an emphasis in applications. In particular, we have studied how to compute the homogeneous vanishing ideal of any finite set of points of the projective space using the saturation in Paper A. The same can be achieved by saturating with respect to the ideal generated by a polynomial that does not vanish at any of the points considered. Therefore, it would be interesting to study which polynomials do not vanish at some particular sets of points for computing the corresponding vanishing ideal.

We have also studied the vanishing ideal of the set of fixed representatives of a set of projective points in Papers B and C. By obtaining Gröbner bases of these ideals, we have obtained bases for the subfield subcodes of projective Reed-Solomon codes and projective Reed-Muller codes, which have been used to construct EAQECCs with good parameters. Using these Gröbner bases, we obtain the hulls of projective Reed-Muller codes over the projective plane in Paper F. This Gröbner basis approach may be used in the future to study other aspects of projective Reed-Muller codes, such as their weight distribution, which has been an extensive object of study for the affine case.

A different approach to study projective Reed-Muller codes is given in Paper D, where a recursive construction is given. With this construction, we also obtain bases for the subfield subcodes of projective Reed-Muller codes for some particular degrees. Moreover, this recursive construction also provides bounds for the GHWs of projective Reed-Muller codes, allowing the exact determination thereof in many examples. Such recursive constructions have been used for the affine case to obtain decoding algorithms and results about their weight distribution. Moreover, another topic of future research is to investigate whether similar constructions can be obtained for similar families of codes, such as nested projective Cartesian codes [27].

Another topic covered by this thesis are the hulls of projective Reed-Muller codes, which have been determined for the case of the projective plane in Paper E. Furthermore, in Paper F we have also explored ways to change the dimension of the hull by using monomially equivalent codes, giving rise to EAQECCs with flexible amounts of entanglement. As before, a future research agenda would be to study if this computations can be carried out for other families of codes.

As we have mentioned in the previous paragraphs, one of the main contributions of this thesis is to fill some of the gaps in knowledge between affine and projective Reed-Muller codes, in particular with respect to their subfield subcodes, hulls and generalized Hamming weights. Nevertheless, some of these topics are still wide open, such as the determination of the hulls for arbitrary projective Reed-Muller codes, and the exact determination of their generalized Hamming weights.

In Paper H we have given lower and upper bounds for the GHWs of MPCs, focusing on the cases with two and three constituent codes. As an application of these bounds, we get the exact value of the GHWs of the MPCs obtained by using two Reed-Solomon codes. The techniques used are inspired by the ones considered with the recursive construction from Paper D for projective Reed-Muller codes. Some of these techniques can be generalized to obtain bounds for the relative generalized Hamming weights of matrix-product codes, which could have applications for secret sharing schemes and quantum codes.

Finally, with respect to quantum fault-tolerant computing, we have given a manageable characterization of CSS-T quantum codes in Paper G. With this new view on CSS-T codes, we have obtained a propagation rule and we have determined the pairs of cyclic codes that give rise to CSS-T codes. This opens the path to considering other families of binary codes to construct CSS-T codes. A more ambitious project would be to obtain similar conditions for a certain non-Clifford operator (analogous to the T gate) in the p-ary case (instead of binary). This would greatly increase the families of classical codes we can consider to construct codes suitable for fault-tolerant computing, which in turn may give better parameters. Triorthogonal codes are a particular case of CSS-T codes which has aroused a lot of attention recently. Finding alternative characterizations for these codes, and obtaining new constructions using cyclic codes (or subfield subcodes of evaluation codes) is also a natural future research project.

Global bibliography

[1] J. Abbott, A. M. Bigatti, and L. Robbiano. CoCoA: a system for doing Computations in Commutative Algebra. Available at `http://cocoa.dima.unige.it`.

[2] J. T. Anderson, G. Duclos-Cianci, and D. Poulin. Fault-tolerant conversion between the Steane and Reed-Muller quantum codes. *Phys. Rev. Lett.*, 113:080501, Aug 2014.

[3] S. E. Anderson, E. Camps-Moreno, H. H. López, G. L. Matthews, D. Ruano, and I. Soprunov. Relative hulls and quantum codes. *IEEE Trans. Inform. Theory*, 70(5):3190–3201, 2024.

[4] E. Andrade, J. Bolkema, T. Dexter, H. Eggers, V. Luongo, F. Manganiello, and L. Szramowski. CSS-T codes from Reed Muller codes for quantum fault tolerance. *ArXiv 2305.06423*, 2023.

[5] S. Ball. Some constructions of quantum MDS codes. *Des. Codes Cryptogr.*, 89(5):811–821, 2021.

[6] T. Ball, E. Camps, H. Chimal-Dzul, D. Jaramillo-Velez, H. López, N. Nichols, M. Perkins, I. Soprunov, G. Vera-Martínez, and G. Whieldon. Coding theory package for Macaulay2. *J. Softw. Algebra Geom.*, 11(1):113–122, 2021.

[7] A. I. Barbero and C. Munuera. The weight hierarchy of Hermitian codes. *SIAM J. Discrete Math.*, 13(1):79–104, 2000.

[8] P. Beelen and M. Datta. Generalized Hamming weights of affine Cartesian codes. *Finite Fields Appl.*, 51:130–145, 2018.

[9] P. Beelen, M. Datta, and S. R. Ghorpade. Maximum number of common zeros of homogeneous polynomials over finite fields. *Proc. Amer. Math. Soc.*, 146(4):1451–1468, 2018.

[10] P. Beelen, M. Datta, and S. R. Ghorpade. Vanishing ideals of projective spaces over finite fields and a projective footprint bound. *Acta Math. Sin. (Engl. Ser.)*, 35(1):47–63, 2019.

[11] P. Beelen, M. Datta, and S. R. Ghorpade. A combinatorial approach to the number of solutions of systems of homogeneous polynomial equations over finite fields. *Mosc. Math. J.*, 22(4):565–593, 2022.

[12] E. Berardini, A. Caminata, and A. Ravagnani. Structure of CSS and CSS-T quantum codes. *Des. Codes Cryptogr.*, 2024.

[13] J. Bierbrauer. The theory of cyclic codes and a generalization to additive codes. *Des. Codes Cryptogr.*, 25(2):189–206, 2002.

[14] J. Bierbrauer and Y. Edel. New code parameters from Reed-Solomon subfield codes. *IEEE Trans. Inform. Theory*, 43(3):953–968, 1997.

[15] J. Bierbrauer and Y. Edel. Quantum twisted codes. *J. Combin. Des.*, 8(3):174–188, 2000.

[16] T. Blackmore and G. H. Norton. Matrix-product codes over $\mathbb{F}_q$. *Appl. Algebra Engrg. Comm. Comput.*, 12(6):477–500, 2001.

[17] M. Boguslavsky. On the number of solutions of polynomial systems. *Finite Fields Appl.*, 3(4):287–299, 1997.

[18] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[19] S. Bravyi and J. Haah. Magic-state distillation with low overhead. *Phys. Rev. A*, 86:052329, Nov 2012.

[20] S. Bravyi and A. Kitaev. Universal quantum computation with ideal Clifford gates and noisy ancillas. *Phys. Rev. A (3)*, 71(2):022316, 14, 2005.

[21] T. Brun, I. Devetak, and M.-H. Hsieh. Correcting quantum errors with entanglement. *Science*, 314(5798):436–439, 2006.

[22] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane. Quantum error correction via codes over GF(4). *IEEE Trans. Inform. Theory*, 44(4):1369–1387, 1998.

[23] A. R. Calderbank and P. W. Shor. Good quantum error-correcting codes exist. *Phys. Rev. A*, 54:1098–1105, Aug 1996.

[24] E. Camps-Moreno, I. García-Marco, H. H. López, I. Márquez-Corbella, E. Martínez-Moro, and E. Sarmiento. On the generalized Hamming weights of hyperbolic codes. *J. Algebra Appl.*, 23(7):Paper No. 2550062, 18, 2024.

[25] E. Camps-Moreno, H. H. López, G. L. Matthews, D. Ruano, R. San-José, and I. Soprunov. An algebraic characterization of binary CSS-T codes and cyclic CSS-T codes for quantum fault tolerance. *Quantum Inf. Process.*, 23(230), 2024.

[26] E. Camps-Moreno, H. H. López, G. L. Matthews, D. Ruano, R. San-José, and I. Soprunov. Parity check matrices for the codes in "An algebraic characterization of binary CSS-T codes and cyclic CSS-T codes for quantum fault tolerance". GitHub repository. Available online: `https://github.com/RodrigoSanJose/Cyclic-CSS-T`, 2024. Accessed on 18 April 2024.

[27] C. Carvalho, V. G. L. Neumann, and H. H. López. Projective nested cartesian codes. *Bull. Braz. Math. Soc. (N.S.)*, 48(2):283–302, 2017.

[28] C. Carvalho, X. Ramírez-Mondragón, V. G. L. Neumann, and H. Tapia-Recillas. Projective Reed-Muller type codes on higher dimensional scrolls. *Des. Codes Cryptogr.*, 87(9):2027–2042, 2019.

[29] I. Cascudo. On squares of cyclic codes. *IEEE Trans. Inform. Theory*, 65(2):1034–1047, 2019.

[30] I. Cascudo, J. S. Gundersen, and D. Ruano. Squares of matrix-product codes. *Finite Fields Appl.*, 62:101606, 21, 2020.

[31] H. Chen. On the hull-variation problem of equivalent linear codes. *IEEE Trans. Inform. Theory*, 69(5):2911–2922, 2023.

[32] S. D. Cohen. Primitive elements and polynomials with arbitrary trace. *Discrete Math.*, 83(1):1–7, 1990.

[33] S. M. Cooper, A. Seceleanu, Ş. O. Tohăneanu, M. V. Pinto, and R. H. Villarreal. Generalized minimum distance functions and algebraic invariants of Geramita ideals. *Adv. in Appl. Math.*, 112:101940, 34, 2020.

[34] D. A. Cox, J. Little, and D. O'Shea. *Ideals, varieties, and algorithms*. Undergraduate Texts in Mathematics. Springer, Cham, fourth edition, 2015. An introduction to computational algebraic geometry and commutative algebra.

[35] S. X. Cui, D. Gottesman, and A. Krishna. Diagonal gates in the Clifford hierarchy. *Phys. Rev. A*, 95(1):012329, 7, 2017.

[36] M. Datta and S. R. Ghorpade. Number of solutions of systems of homogeneous polynomial equations over finite fields. *Proc. Amer. Math. Soc.*, 145(2):525–541, 2017.

[37] W. Decker, G.-M. Greuel, G. Pfister, and H. Schönemann. SINGULAR 4-4-0 — A computer algebra system for polynomial computations. `http://www.singular.uni-kl.de`, 2024.

[38] P. Delsarte. On subfield subcodes of modified Reed-Solomon codes. *IEEE Trans. Inform. Theory*, IT-21(5):575–576, 1975.

[39] P. Delsarte, J.-M. Goethals, and F. J. MacWilliams. On generalized Reed-Muller codes and their relatives. *Information and Control*, 16:403–442, 1970.

[40] I. M. Duursma, C. Rentería, and H. Tapia-Recillas. Reed-Muller codes on complete intersections. *Appl. Algebra Engrg. Comm. Comput.*, 11(6):455–462, 2001.

[41] B. Eastin and E. Knill. Restrictions on transversal encoded quantum gate sets. *Phys. Rev. Lett.*, 102:110502, Mar 2009.

[42] D. Eisenbud. *Commutative algebra*, volume 150 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1995. With a view toward algebraic geometry.

[43] B. Engheta. On the projective dimension and the unmixed part of three cubics. *J. Algebra*, 316(2):715–734, 2007.

[44] K. Feng and Z. Ma. A finite Gilbert-Varshamov bound for pure stabilizer quantum codes. *IEEE Trans. Inform. Theory*, 50(12):3323–3325, 2004.

[45] C. Galindo, O. Geil, F. Hernando, and D. Ruano. On the distance of stabilizer quantum codes from J-affine variety codes. *Quantum Inf. Process.*, 16(4):Paper No. 111, 32, 2017.

[46] C. Galindo, O. Geil, F. Hernando, and D. Ruano. New binary and ternary LCD codes. *IEEE Trans. Inform. Theory*, 65(2):1008–1016, 2019.

[47] C. Galindo and F. Hernando. Quantum codes from affine variety codes and their subfield-subcodes. *Des. Codes Cryptogr.*, 76(1):89–100, 2015.

[48] C. Galindo, F. Hernando, R. Matsumoto, and D. Ruano. Entanglement-assisted quantum error-correcting codes over arbitrary finite fields. *Quantum Inf. Process.*, 18(4):Paper No. 116, 18, 2019.

[49] C. Galindo, F. Hernando, R. Matsumoto, and D. Ruano. Asymmetric entanglement-assisted quantum error-correcting codes and bch codes. *IEEE Access*, 8:18571–18579, 2020.

[50] C. Galindo, F. Hernando, C. Munuera, and D. Ruano. Locally recoverable codes from the matrix-product construction. *ArXiv 2310.15703*, 2023.

[51] C. Galindo, F. Hernando, and D. Ruano. New quantum codes from evaluation and matrix-product codes. *Finite Fields Appl.*, 36:98–120, 2015.

[52] C. Galindo, F. Hernando, and D. Ruano. Stabilizer quantum codes from J-affine variety codes and a new Steane-like enlargement. *Quantum Inf. Process.*, 14(9):3211–3231, 2015.

[53] C. Galindo, F. Hernando, and D. Ruano. Classical and quantum evaluation codes at the trace roots. *IEEE Trans. Inform. Theory*, 65(4):2593–2602, 2019.

[54] C. Galindo, F. Hernando, and D. Ruano. Entanglement-assisted quantum error-correcting codes from RS codes and BCH codes with extension degree 2. *Quantum Inf. Process.*, 20(5):Paper No. 158, 26, 2021.

[55] S. R. Ghorpade. A note on Nullstellensatz over finite fields. In *Contributions in algebra and algebraic geometry*, volume 738 of *Contemp. Math.*, pages 23–32. Amer. Math. Soc., 2019.

[56] S. R. Ghorpade and R. Ludhani. On the minimum distance, minimum weight codewords, and the dimension of projective Reed-Muller codes. *Adv. Math. Commun.*, 18(2):360–382, 2024.

[57] P. Gimenez, D. Ruano, and R. San-José. Entanglement-assisted quantum error-correcting codes from subfield subcodes of projective Reed-Solomon codes. *Comput. Appl. Math.*, 42(8):Paper No. 363, 31, 2023.

[58] P. Gimenez, D. Ruano, and R. San-José. Saturation and vanishing ideals. *São Paulo J. Math. Sci.*, 17(1):147–155, 2023.

[59] P. Gimenez, D. Ruano, and R. San-José. Subfield subcodes of projective Reed-Muller codes. *Finite Fields Appl.*, 94:Paper No. 102353, 46, 2024.

[60] M. González-Sarabia, J. Martínez-Bernal, R. H. Villarreal, and C. E. Vivares. Generalized minimum distance functions. *J. Algebraic Combin.*, 50(3):317–346, 2019.

[61] M. González-Sarabia and C. Rentería. The dual code of some Reed-Muller type codes. *Appl. Algebra Engrg. Comm. Comput.*, 14(5):329–333, 2004.

[62] P. Gopalan, V. Guruswami, and P. Raghavendra. List decoding tensor products and interleaved codes. *SIAM J. Comput.*, 40(5):1432–1462, 2011.

[63] D. Gottesman. The Heisenberg representation of quantum computers. In *Group22: Proceedings of the XXII International Colloquium in Group Theoretical Methods in Physics (Hobart, 1998)*, pages 32–43. Int. Press, Cambridge, MA, 1999.

[64] M. Grassl. Bounds on the minimum distance of linear codes and quantum codes. Online available at `http://www.codetables.de`, 2007. Accessed on 2023-04-04.

[65] M. Grassl. Algebraic quantum codes: linking quantum mechanics and discrete mathematics. *International Journal of Computer Mathematics: Computer Systems Theory*, 6(4):243–259, 2021.

[66] M. Grassl. New quantum codes from CSS codes. *Quantum Inf. Process.*, 22(1):Paper No. 86, 11, 2023.

[67] D. R. Grayson and M. E. Stillman. Macaulay2, a software system for research in algebraic geometry.

[68] G.-M. Greuel and G. Pfister. *A* **Singular** *introduction to commutative algebra*. Springer, Berlin, extended edition, 2008. With contributions by Olaf Bachmann, Christoph Lossen and Hans Schönemann.

[69] V. Guruswami. List decoding from erasures: bounds and code constructions. *IEEE Trans. Inform. Theory*, 49(11):2826–2833, 2003.

[70] M. B. Hastings and J. Haah. Distillation with sublogarithmic overhead. *Phys. Rev. Lett.*, 120:050504, Jan 2018.

[71] M. Hattori, R. J. McEliece, and G. Solomon. Subspace subcodes of Reed-Solomon codes. *IEEE Trans. Inform. Theory*, 44(5):1861–1880, 1998.

[72] P. Heijnen and R. Pellikaan. Generalized Hamming weights of q-ary Reed-Muller codes. *IEEE Trans. Inform. Theory*, 44(1):181–196, 1998.

[73] F. Hernando, T. Høholdt, and D. Ruano. List decoding of matrix-product codes from nested codes: an application to quasi-cyclic codes. *Adv. Math. Commun.*, 6(3):259–272, 2012.

[74] F. Hernando, K. Lally, and D. Ruano. Construction and decoding of matrix-product codes from nested codes. *Appl. Algebra Engrg. Comm. Comput.*, 20(5-6):497–507, 2009.

[75] F. Hernando, K. Marshall, and M. E. O'Sullivan. The dimension of subcode-subfields of shortened generalized Reed-Solomon codes. *Des. Codes Cryptogr.*, 69(1):131–142, 2013.

[76] F. Hernando, M. E. O'Sullivan, E. Popovici, and S. Srivastava. Subfield-subcodes of generalized toric codes. In *2010 IEEE International Symposium on Information Theory*, pages 1125–1129, 2010.

[77] F. Hernando and D. Ruano. Decoding of matrix-product codes. *J. Algebra Appl.*, 12(4):1250185, 15, 2013.

[78] W. C. Huffman and V. Pless. *Fundamentals of error-correcting codes*. Cambridge University Press, Cambridge, 2003.

[79] L. Ioffe and M. Mézard. Asymmetric quantum error-correcting codes. *Phys. Rev. A*, 75:032345, Mar 2007.

[80] D. Jaramillo, M. Vaz Pinto, and R. H. Villarreal. Evaluation codes and their basic parameters. *Des. Codes Cryptogr.*, 89(2):269–300, 2021.

[81] S. Jitman and T. Mankean. Matrix-product constructions for Hermitian self-orthogonal codes. *Chamchuri J. Math.*, 9:35–51, 2017.

[82] N. Kaplan and J.-L. Kim. Hulls of Projective Reed-Muller Codes. *ArXiv 2406.04757*, 2024.

[83] T. Kasami, S. Lin, and W. W. Peterson. New generalizations of the Reed-Muller codes. I. Primitive codes. *IEEE Trans. Inform. Theory*, IT-14:189–199, 1968.

[84] A. Ketkar, A. Klappenecker, S. Kumar, and P. K. Sarvepalli. Nonbinary stabilizer codes over finite fields. *IEEE Trans. Inform. Theory*, 52(11):4892–4914, 2006.

[85] M. Kreuzer and L. Robbiano. *Computational commutative algebra. 1.* Springer-Verlag, Berlin, 2000.

[86] M. Kreuzer and L. Robbiano. *Computational commutative algebra. 2.* Springer-Verlag, Berlin, 2005.

[87] G. G. La Guardia. *Quantum error correction—symmetric, asymmetric, synchronizable, and convolutional codes*. Quantum Science and Technology. Springer, Cham, 2020.

[88] G. Lachaud. Projective Reed-Muller codes. In *Coding theory and applications (Cachan, 1986)*, volume 311 of *Lecture Notes in Comput. Sci.*, pages 125–129. Springer, Berlin, 1988.

[89] G. Lachaud. The parameters of projective Reed-Muller codes. *Discrete Math.*, 81(2):217–221, 1990.

[90] H. H. López, I. Soprunov, and R. H. Villarreal. The dual of an evaluation code. *Des. Codes Cryptogr.*, 89(7):1367–1403, 2021.

[91] G. Luo, M. F. Ezerman, M. Grassl, and S. Ling. Constructing quantum error-correcting codes that require a variable amount of entanglement. *Quantum Inf. Process.*, 23(1):Paper No. 4, 28, 2024.

[92] G. Luo, M. F. Ezerman, and S. Ling. Three new constructions of optimal locally repairable codes from matrix-product codes. *IEEE Trans. Inform. Theory*, 69(1):75–85, 2023.

[93] G. Luo, M. F. Ezerman, S. Ling, and X. Pan. New families of MDS symbol-pair codes from matrix-product codes. *IEEE Trans. Inform. Theory*, 69(3):1567–1587, 2023.

[94] J. MacWilliams. Error-correcting codes for multiple-level transmission. *Bell System Tech. J.*, 40:281–308, 1961.

[95] T. Mankean and S. Jitman. Matrix-product constructions for self-orthogonal linear codes. In *2016 12th International Conference on Mathematics, Statistics, and Their Applications (ICMSA)*, pages 6–10, 2016.

[96] J. Martínez-Bernal, Y. Pitones, and R. H. Villarreal. Minimum distance functions of graded ideals and Reed-Muller-type codes. *J. Pure Appl. Algebra*, 221(2):251–275, 2017.

[97] J. Martínez-Bernal, Y. Pitones, and R. H. Villarreal. Minimum distance functions of graded ideals and Reed-Muller-type codes. *J. Pure Appl. Algebra*, 221(2):251–275, 2017.

[98] R. Matsumoto. Improved Gilbert–Varshamov bound for Entanglement-Assisted Asymmetric Quantum Error Correction by Symplectic Orthogonality. *IEEE Trans. Quantum Eng.*, 1:1–4, 2020.

[99] D.-J. Mercier and R. Rolland. Polynômes homogènes qui s'annulent sur l'espace projectif $\mathrm{P}^m(\mathbf{F}_q)$. *J. Pure Appl. Algebra*, 124(1-3):227–240, 1998.

[100] C. Munuera. On the generalized Hamming weights of geometric Goppa codes. *IEEE Trans. Inform. Theory*, 40(6):2092–2099, 1994.

[101] N. Nakashima and H. Matsui. Decoding of projective reed-muller codes by dividing a projective space into affine spaces. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, E99.A(3):733–741, 2016.

[102] L. P. Natarajan and P. Krishnan. Berman codes: a generalization of Reed-Muller codes that achieve BEC capacity. *IEEE Trans. Inform. Theory*, 69(11):6956–6980, 2023.

[103] G. Nebe, E. M. Rains, and N. J. A. Sloane. The invariants of the Clifford groups. *Des. Codes Cryptogr.*, 24(1):99–121, 2001.

[104] G. Nebe, E. M. Rains, and N. J. A. Sloane. *Self-dual codes and invariant theory*, volume 17 of *Algorithms and Computation in Mathematics*. Springer-Verlag, Berlin, 2006.

[105] S. Nezami and J. Haah. Classification of small triorthogonal codes. *Phys. Rev. A*, 106(1):Paper No. 012437, 13, 2022.

[106] F. Özbudak and H. Stichtenoth. Note on Niederreiter-Xing's propagation rule for linear codes. *Appl. Algebra Engrg. Comm. Comput.*, 13(1):53–56, 2002.

[107] R. Pellikaan, X.-W. Wu, S. Bulygin, and R. Jurrius. *Codes, cryptology and curves with computer algebra*. Cambridge University Press, Cambridge, 2018.

[108] D.-X. Quan, L.-L. Zhu, C.-X. Pei, and B. C. Sanders. Fault-tolerant conversion between adjacent Reed-Muller quantum codes based on gauge fixing. *J. Phys. A*, 51(11):115305, 16, 2018.

[109] E. M. Rains. Nonbinary quantum codes. *IEEE Trans. Inform. Theory*, 45(6):1827–1832, 1999.

[110] H. Randriambololona. On products and powers of linear codes under componentwise multiplication. In *Algorithmic arithmetic, geometry, and coding theory*, volume 637 of *Contemp. Math.*, pages 3–78. Amer. Math. Soc., Providence, RI, 2015.

[111] N. Rengaswamy, R. Calderbank, M. Newman, and H. D. Pfister. Classical coding problem from transversal T gates. In *2020 IEEE International Symposium on Information Theory (ISIT)*, pages 1891–1896, 2020.

[112] N. Rengaswamy, R. Calderbank, M. Newman, and H. D. Pfister. On optimality of CSS codes for transversal T. *IEEE J. Sel. Areas Inf. Theory*, 1(2):499–514, 2020.

[113] C. Rentería and H. Tapia-Recillas. Reed-Muller codes: an ideal theory approach. *Comm. Algebra*, 25(2):401–413, 1997.

[114] C. Rentería-Márquez, A. Simis, and R. H. Villarreal. Algebraic methods for parameterized codes and invariants of vanishing ideals over finite fields. *Finite Fields Appl.*, 17(1):81–104, 2011.

[115] D. Ruano and R. San-José. Hulls of projective Reed-Muller codes over the projective plane. *SIAM Journal on Applied Algebra and Geometry, to appear. ArXiv 2312.13921*, 2024.

[116] D. Ruano and R. San-José. Quantum error-correcting codes from projective Reed-Muller codes and their hull variation problem. *ArXiv 2312.15308*, 2024.

[117] R. San-José. About the generalized Hamming weights of matrix-product codes. *ArXiv 2407.11810*, 2024.

[118] R. San-José. A recursive construction for projective Reed-Muller codes. *IEEE Transactions on Information Theory, to appear. ArXiv 2312.05072*, 2024.

[119] P. Sarvepalli and A. Klappenecker. Nonbinary quantum reed-muller codes. In *Proceedings. International Symposium on Information Theory, 2005. ISIT 2005.*, pages 1023–1027, 2005.

[120] P. K. Sarvepalli, S. A. Aly, and A. Klappenecker. Nonbinary stabilizer codes. In *Mathematics of quantum computation and quantum technology*, Chapman & Hall/CRC Appl. Math. Nonlinear Sci. Ser., pages 287–308. Chapman & Hall/CRC, Boca Raton, FL, 2008.

[121] P. K. Sarvepalli, A. Klappenecker, and M. Rötteler. Asymmetric quantum codes: constructions, bounds and performance. *Proc. R. Soc. Lond. Ser. A Math. Phys. Eng. Sci.*, 465(2105):1645–1672, 2009.

[122] P. Shor. Fault-tolerant quantum computation. In *Proceedings of 37th Conference on Foundations of Computer Science*, pages 56–65, 1996.

[123] P. W. Shor. Scheme for reducing decoherence in quantum computer memory. *Phys. Rev. A*, 52:R2493–R2496, Oct 1995.

[124] P. W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comput.*, 26(5):1484–1509, 1997.

[125] A. B. Sørensen. Projective Reed-Muller codes. *IEEE Trans. Inform. Theory*, 37(6):1567–1576, 1991.

[126] A. B. Sørensen. A note on a gap in the proof of the minimum distance for projective Reed-Muller codes. *ArXiv 2310.03574*, 2023.

[127] A. Steane. Multiple-Particle Interference and Quantum Error Correction. *Proceedings of the Royal Society of London Series A*, 452(1954):2551–2577, Nov. 1996.

[128] A. M. Steane. Simple quantum error-correcting codes. *Phys. Rev. A (3)*, 54(6):4741–4751, 1996.

[129] A. M. Steane. Quantum Reed-Muller codes. *IEEE Trans. Inform. Theory*, 45(5):1701–1703, 1999.

[130] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 10.3)*, 2023. `https://www.sagemath.org`.

[131] Ş. O. Tohăneanu. *Commutative Algebra Methods for Coding Theory*. De Gruyter, Berlin, Boston, 2024.

[132] V. K. Wei. Generalized Hamming weights for linear codes. *IEEE Trans. Inform. Theory*, 37(5):1412–1418, 1991.